暗号資産関連業者における
サイバーセキュリティの課題と対策に関する研究調査

2026年6月30日

合同会社デロイト トーマツ

謝辞・免責事項

謝辞

■本報告書作成にあたり、京都大学・岩下直行名誉教授、米ジョージタウン大学・松尾真一郎研究教授より有益な助言及びコメントをいただいたほか、日本銀行、デジタル庁のオブザーバー、ならびに金融庁のご担当者からも、有益な示唆・助言を頂きました

■Fireblocks, タレスDISジャパン株式会社, DFNS社などに個別にヒアリングさせて頂いた内容の一部を掲載しています

■そのほか、インシデントの詳細について一部関連業者にヒアリングさせて頂き、有益な情報提供をいただきました

■2026年2月、Japan Fintech Week2026中に開催されたJFSA Blockchain Roundtableにて、参加された有識者より助言をいただきました
2026年3月、Blockchain Governance Initiative Network (BGIN) Block#14会合においても、参加された有識者より助言をいただきました

■もっとも、本報告書の内容に関する誤りは、すべて受託者である合同会社デロイト トーマツに帰します

免責事項

■ 本報告書の内容は金融庁の公式見解を示すものではありません

■ 本報告書で記載している内容のうち、過去または現在の事実以外の事項は、本報告書の執筆時点で入手可能な情報に基づく見通しであり、実際の動向等は、種々の不確定要因により変動する可能性があります

■ 本報告書における事例分析の記載は、各事例に関して公表されている資料及び本報告書の執筆時点で入手可能な情報に基づき調査研究の目的から整理したもので、個別事案に関する責任の所在又は法的評価を示すものではありません

調査状況を定例会合で報告・討議し、有識者の助言を調査に反映させた上で、報告書を取り纏めた

調査研究の進め方

調査研究

- 包括的な業界構造の実態調査
- 事例分析
- 暗号資産特有リスクの分析

■ 業界構造は、中央集権型取引所（Centralized Exchange, CEX）を中核に、関係事業者をサプライチェーンとして捉え、関係者間の依存関係を可視化した

■ 事例分析は、カテゴリ別に代表事例を数件選択し、実施した

討議

反映

定例会合

1. 定義と分類及びサプライチェーン可視化
2. 事例集の作成と基準分析
3. セキュリティ対策の整理
4. リスク要因調査および委託管理の整理
5. 取り纏め報告書

取り纏め

報告書

国際カンファレンス及び国際的な意見発信への貢献

※「BGIN（Blockchain Governance Initiative Network）Block 14」および「Japan Fintech Week 2026 Blockchain Roundtable」で実施

頻発するサイバー攻撃と委託起因の脆弱性を受け、サプライチェーン可視化とリスク整理をし、包括的なサイバーセキュリティ態勢整備・対策の強化案を整理する

研究の背景・目的

■ 近年、中央集権型取引所や分散型金融プロトコルを標的としたサイバー攻撃が頻発し、多数の暗号資産流出事案が発生している。特に、署名鍵の盗難に限らず、第三者委託に起因するサイバーセキュリティ上の課題が顕在化しており、攻撃手法は一層巧妙化している。こうした状況を踏まえ、署名鍵管理にとどまらず、業界全体を対象とした包括的なサイバーセキュリティ態勢整備と対策の強化が不可欠となっている

■ 本調査は、暗号資産業界におけるプレイヤー構造および委託関係を把握し、過去のサイバー攻撃事例を既存のサイバーセキュリティ基準と照合して、リスクと対応策を整理することで、監督・指導に資する知見を得ることを目的とする。具体的には、①「暗号資産交換業等におけるサイバーセキュリティ強化に向けた取組方針」の趣旨も踏まえ、暗号資産交換業者向け事務ガイドラインで求めるサイバーセキュリティ水準の引上げに向けて、不足点の拡充や交換業者がより意識すべき項目に係る検討を行う。加えて、契約管理や監査態勢等の実務的視点から対応策を整理し、事務ガイドライン改訂に向けた知見を得る。併せて、②業者・当局間の連携を促進する一助とするほか、暗号資産業界におけるサイバーセキュリティ強化が国際的な課題であることを踏まえ、国際的議論の基盤となることを期待する。また、③交換業者が標準やガイドラインを活用して適切なセキュリティ態勢を構築できるよう、サプライチェーンやシステムの脆弱性を把握し、講ずべき具体的対策を明らかにする。

■ 本調査研究で実施した項目

1. **暗号資産業界におけるサプライチェーンとそのリスクの把握**
   暗号資産業界における主要なプレイヤーを整理し、役割や業務内容を明確化する。併せて第三者委託先との関係性を可視化し、
   業務委託や技術連携の構造を把握する
2. **事例分析**
   国内外の代表的なサイバー攻撃事例について、攻撃手法や突かれた脆弱性を整理する。NIST CSF 2.0、FISC 安全対策基準、
   金融庁サイバーセキュリティガイドライン等の国際的・国内的な標準・ガイドラインを踏まえて、
   攻撃を受けた業者等が講ずべきだった対策のほか、既存ガイドラインではカバーしきれなかったリスクを分析する
3. **暗号資産特有リスクの分析**
   暗号資産業者に特有の新たなリスク要因を分析する。特に、第三者委託先との契約管理、監査体制、サイバーセキュリティ検証手法等、
   実務的な観点からの対応策を検討し、既存ガイドラインの拡張に資する知見を得る。これにより、暗号資産業者のサイバーセキュリティ体制強化と
   金融行政における監督・指導の高度化への貢献を目指す

目次構成

用語集

用語	定義	
AML／CFT	Anti-Money Laundering and Combating the Financing of Terrorism	マネー・ローンダリング及びテロ資金供与対策
BIS	Bank for International Settlements	国際決済銀行
BPT	Balancer Pool Token	バランサー・プール・トークン
CCSS	CryptoCurrency Security Standard	暗号資産セキュリティ標準
CDN	Content Delivery Network	コンテンツ配信ネットワーク
CEX	Centralized Exchange	暗号資産取引所
CGTF	Crypto Governance Task Force	暗号資産（暗号）ガバナンス・タスクフォース
CICD	Continuous Integration／Continuous Delivery (or Deployment)	継続的インテグレーション／継続的デリバリ（またはデプロイ）
DAO	Decentralized Autonomous Organization	分散型自律組織
DeFi	Decentralized Finance	分散型金融
DEX	Decentralized Exchange	分散型取引所
DNS	Domain Name System	ドメイン・ネーム・システム
DoS	Denial of Service	サービス妨害
ENISA	European Union Agency for Cybersecurity	欧州連合サイバーセキュリティ機関

用語集

用語	定義	
ERC	Ethereum Request for Comments	イーサリアム技術提案
ETH	Ether (Ethereum)	イーサ（イーサリアム）
FATF	Financial Action Task Force	金融活動作業部会
FSB	Financial Stability Board	金融安定理事会
HSM	Hardware Security Module	ハードウェア・セキュリティ・モジュール
IEC	International Electrotechnical Commission	国際電気標準会議
ISO	International Organization for Standardization	国際標準化機構
LP	Liquidity Provider／Liquidity Pool	流動性提供者／流動性プール（文脈で使い分け）
LST	Liquid Staking Token	リキッド・ステーキング・トークン
LRT	Liquid Restaking Token	リキッド・リステーキング・トークン
MEV	Maximal Extractable Value	最大抽出可能価値
MPC	Multi-Party Computation	マルチパーティ計算（秘密計算）
RAT	Remote Access Trojan	リモートアクセス型トロイの木馬
TVL	Total Value Locked	DeFi に預けられた暗号資産の総額

研究結果サマリ(1/2)

■ 近年、暗号資産関連業者を標的としたサイバー攻撃が継続的に発生・拡大しており、攻撃の手口は年々多様化・高度化・組織化している。特に、AI技術の活用等により脆弱性探索や攻撃経路の特定が高速化する中、委託先への侵害、スマートコントラクトの脆弱性、マルウェア、フィッシング、権限奪取等を組み合わせた攻撃が顕在化している。攻撃者は、システムへの侵入そのものにとどまらず、署名鍵、ウォレット、アクセス制御、CI/CD、クラウドIAM/KMS、署名サービス等の運用インフラストラクチャを標的とする傾向を強めており、**自社システムのみならず外部システムを経由したサプライチェーン攻撃への対応が重要か**

■ ブロックチェーンは、信頼の対象を再定義する技術と期待されてきたが、現実の暗号資産関連サービスは、純粋な分散モデルではなく、**中央集権的な運用主体と分散型基盤の双方のリスクを併せ持つアーキテクチャとして運営されている。この構造的前提を踏まえ**、オンチェーンのコードやプロトコルだけではなく、オフチェーン要素、運用統制、外部依存関係、ガバナンスを含む**包括的なリスク評価を行うことが必要か**

■ 本研究では、被害額が大きい主要な攻撃手法として、**サードパーティへの侵害、スマートコントラクトの脆弱性、ラグプル、フラッシュローン攻撃、マルウェア攻撃**等を取り上げ、近年のDeFiを含む暗号資産関連サービスに対する攻撃事例を分析した。その結果、署名鍵そのものの窃取ではなく、UI、API、CI/CD、未署名トランザクション生成ロジック、本番環境プログラム等を改ざんし、**正規の署名プロセスを悪用して資産流出に至らせる攻撃が確認された。**また、サードパーティにおけるソーシャルエンジニアリング・マルウェア対策、本番環境アクセス管理、プログラム変更管理、署名時検証、スマートコントラクトのアップグレード権限やビジネスロジック検証等に課題があった可能性が示された

研究結果サマリ(2/2)

■ 業界構造の整理及び事例分析を踏まえ、本研究では、導出された攻撃手法・脆弱性と、既存ガイドライン（NIST CSF 2.0、金融庁事務ガイドライン、金融庁サイバーセキュリティガイドライン、FISC安全対策基準、JVCEA規則・標準、OWASP SCSVS等）との比較分析を行った。その結果、既存ガイドラインには主要な脆弱性に対応する項目が存在する一方で、**暗号資産関連業者においては、自社のシステム構成、委託関係、ウォレット・鍵管理方式、DeFi・外部サービス利用状況に応じて、管理策を具体化・深掘りする必要があることが確認された**。これを踏まえ、重点的に検討すべき領域として、「**委託先管理の高度化**」「**不正プログラムの混入・改ざん防止策**」「**暗号資産の不正送金防止に関する措置**」「**スマートコントラクト・DeFiへの対応**」「**外部評価の活用**」の**5項目を抽出**し、考察した

■ 特に、暗号資産関連業者が暗号資産の出庫、署名、鍵管理、ウォレット運用、CI/CD、クラウド基盤等の重要業務に外部委託先を利用する場合には、委託先のシステム構造、管理体制、アクセス権限、再委託関係、ログ監視、インシデント対応、プログラム変更管理等を十分に評価する必要があるか。外部評価や第三者保証報告書を確認する場合も、その対象範囲、評価時点、除外範囲、評価者の適格性、是正状況を確認し、不足部分を補完することが求められるか。また、委託先の侵害が自社サービスや利用者資産に波及することを前提に、追加承認、利用上限、異常検知、自動停止、代替手段等の自衛策を整備することが重要か

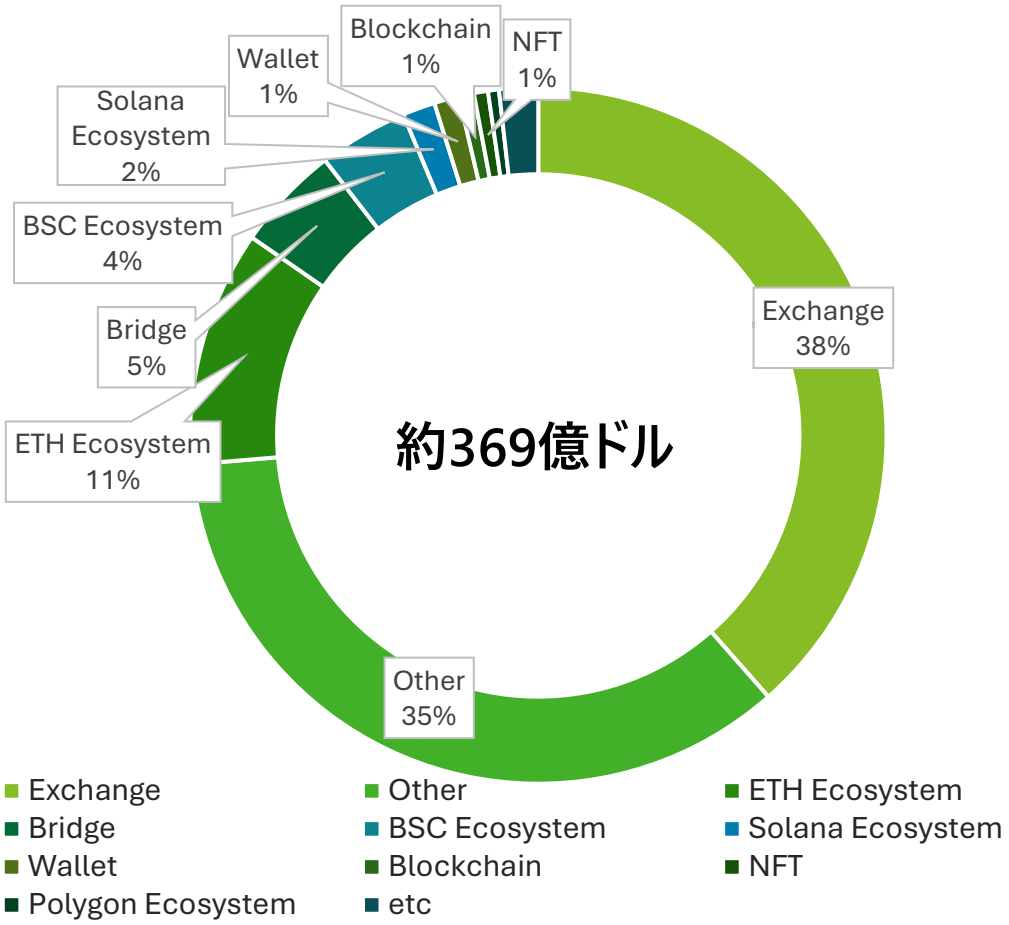
■ また、暗号資産関連業者のサービス水準にもばらつきがある中で、例えば、**暗号資産に関する脅威・脆弱性情報の国際的な共通データ標準の整備**、が重要な検討課題か。さらに、AI時代における脆弱性発見・攻撃経路特定の高速化を踏まえ、アタックサーフェスの削減、インターネットからの分離、開発環境のセキュリティ管理、重要システムの分離、証跡の管理、トレーニング・教育、脆弱性情報開示制度の再設計等の**技術的対策とガバナンスを一体化したサイバーセキュリティ態勢の整備が求められるか**

1. 暗号資産関連のサイバー攻撃の発生状況とリスク評価

1.1 サイバー攻撃事例の傾向

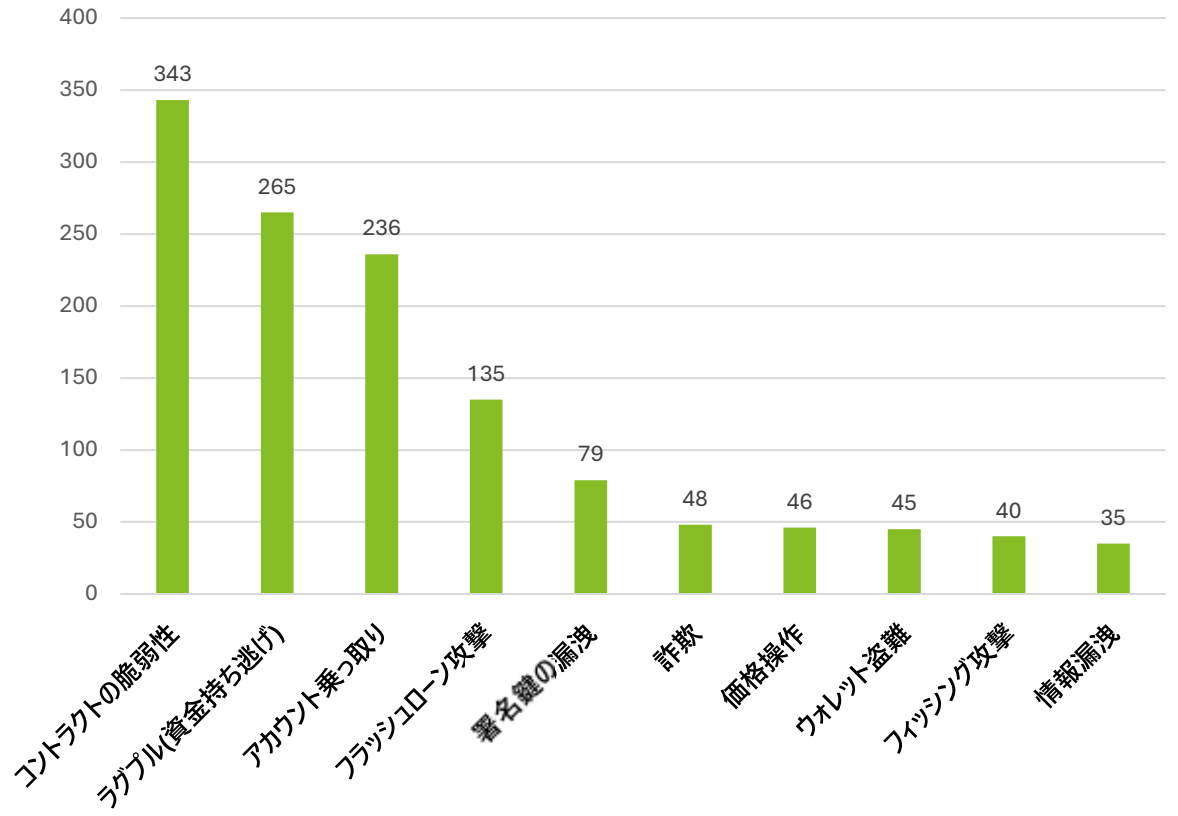
暗号資産関連事業に対する犯罪の手口は多様化している

インシデント別被害額（2012年以降の累計）



*「etc」は、1%以下の各カテゴリを集約したものであり、「Other」は、上記カテゴリ以外の分類不能な項目を指す
参考：「 https://hacked.slowmist.io/en/ 」（SlowMist Hacked）_ 2026年3月時点

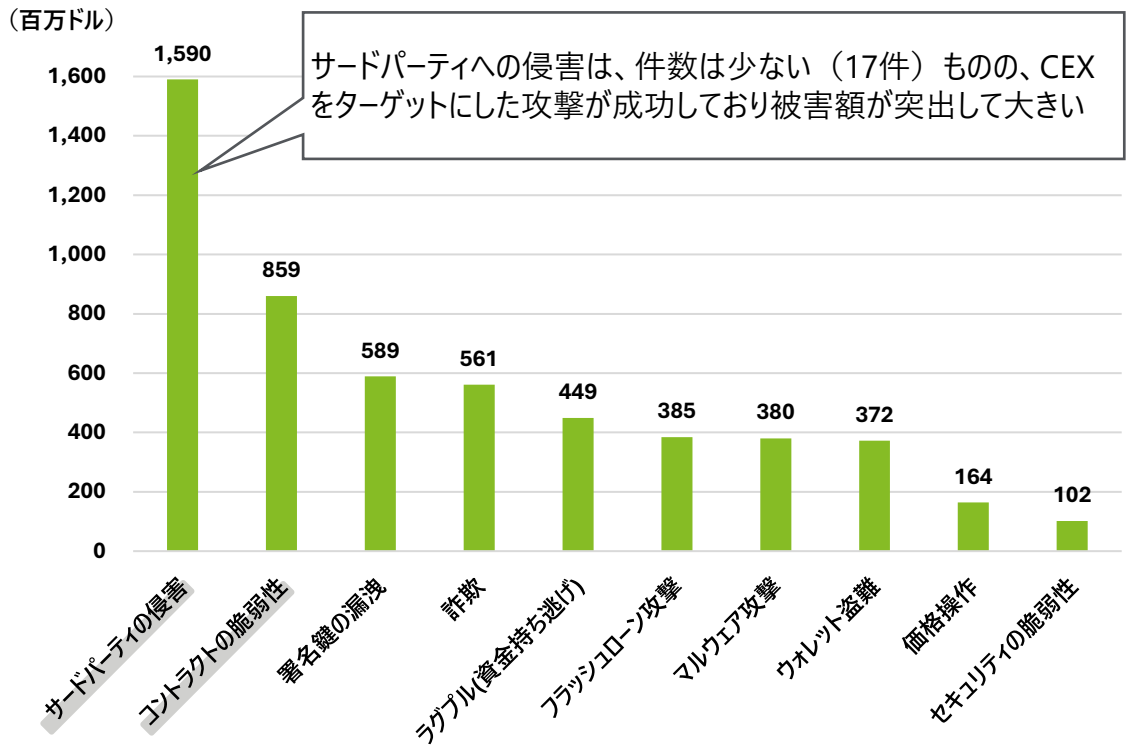
インシデント類別件数（2012年以降の累計）



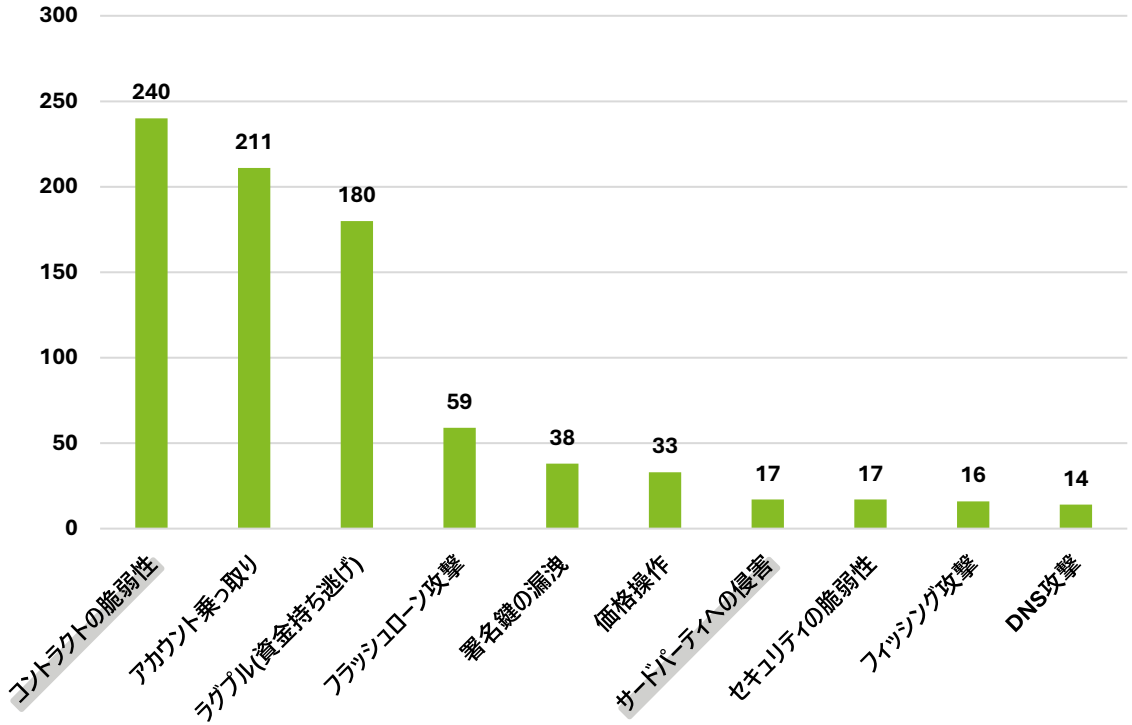
*「ラグプル（資産持ち逃げ）」については、コントラクトの脆弱性等への攻撃を起因とするインシデントも存在するが、サイバーセキュリティの課題ではなく、市場操作や詐欺に関する課題であるものが多い

2023年以降は、サードパーティへの侵害を通じた攻撃や、スマートコントラクトの脆弱性を突いた攻撃の被害が顕著である

インシデント被害額順（2023年以降の累計）



インシデント件数順（2023年以降の累計）

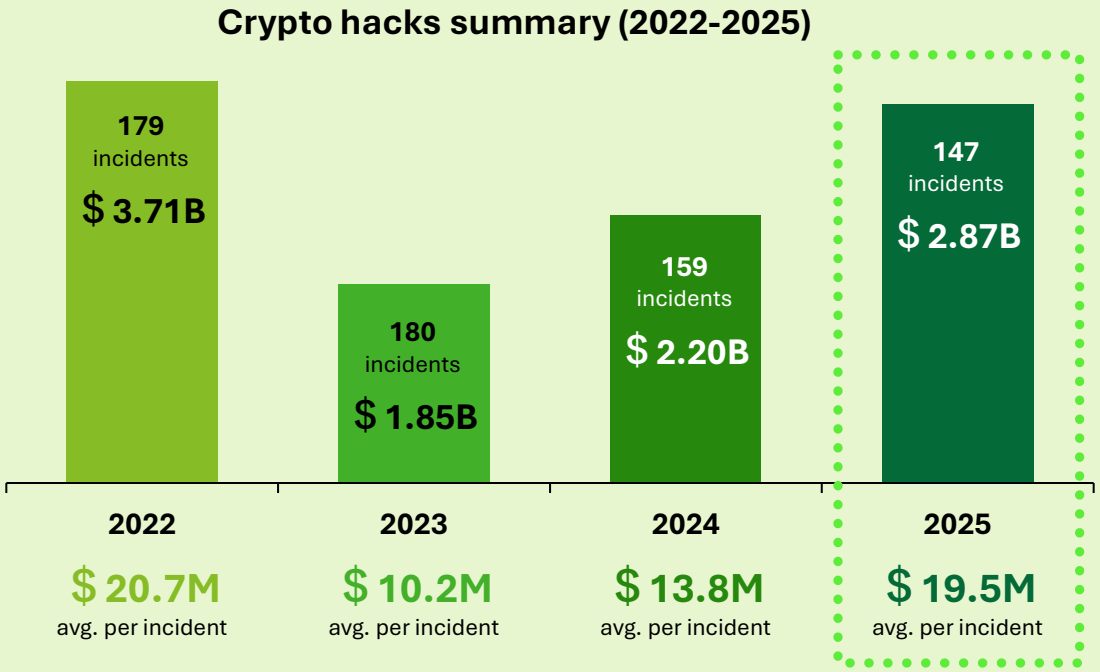


参考：「 https://hacked.slowmist.io/en/ 」（SlowMist Hacked）_ 2026年3月時点

2025年の暗号資産被害額は過去最高となり、一部の大規模インシデントへ被害が極端に集中する傾向がみられる

暗号資産被害に関する直近の動向（1/5）

- TRM Labs社の集計によると、2025年の暗号資産関連の違法取引総額は過去最高の1,580億ドルに達した
- そのうちの28.7億ドルは、約150件のハッキングや脆弱性悪用（エクスプロイト）のインシデントで盗まれたものであり、上位10件のインシデントが年間合計の81%を占める等、大規模インシデントへの被害の集中がみられた



2025年の**インシデント損失金額の平均値は1,950万ドルに増加**したが、中央値は130万ドルに減少した。

2025年2月に発生したBybitの大規模なセキュリティ侵害による損失金額は、年間合計のうち14.6億ドル (51%) を占める。**上位10件のインシデントが年間合計の81%を占める等**、特定プレイヤーへのリスク集中が見られる。

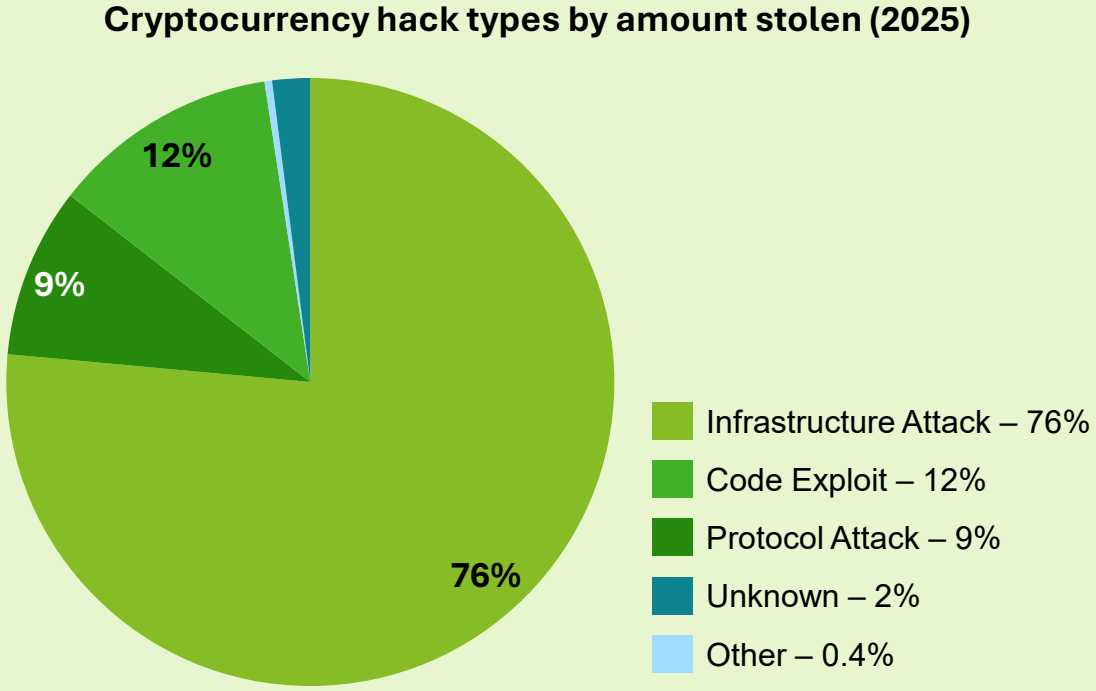
特に国家の支援を受けるハッカーグループに関連する高度な攻撃は、単なるコードの脆弱性悪用にとどまらず、**暗号資産サービスの運営基盤とエコシステムを危険にさらしている。**大量の小規模な事件もエコシステム全体に継続的に発生している。

参考：「2026 Crypto Crime Report – Illicit Crypto Trends & Typologies」（TRM Labs）_2026年2月時点

【一部の大規模インシデントへ被害が極端に集中する要因①】2025年においては、攻撃の標的が投資対効果が高いインフラストラクチャへの直接的な侵害へと移行する傾向が見られた

暗号資産被害に関する直近の動向（2/5）

- 2025年の暗号資産関連インシデントは、件数では近年とほぼ同水準であったが、攻撃手法（ベクトル）の構造的な変化により、損失金額は急激に増加した
- 攻撃の標的は、より上位レイヤーへ移行しており、運用インフラストラクチャ（署名鍵、ウォレット、アクセス制御等）を直接標的にする傾向が強まっている
- 高度な攻撃者にとって、CEX等の中央集権的な事業者の運用インフラストラクチャを侵害することは、最も攻撃対効果が高い手法となっている



2025年に発生したハッキングインシデントを、5つに区分して整理。
- インフラストラクチャ攻撃（Infrastructure Attack）：鍵やサーバー等の運用基盤を直接狙う攻撃
- コードエクスプロイト (Code Exploit)：プログラムの脆弱性やバグを悪用する攻撃
- プロトコル攻撃 (Protocol Attack)：システムの仕様や設計の欠陥を突く攻撃
- 未知 (Unknown)
- その他 (Other)

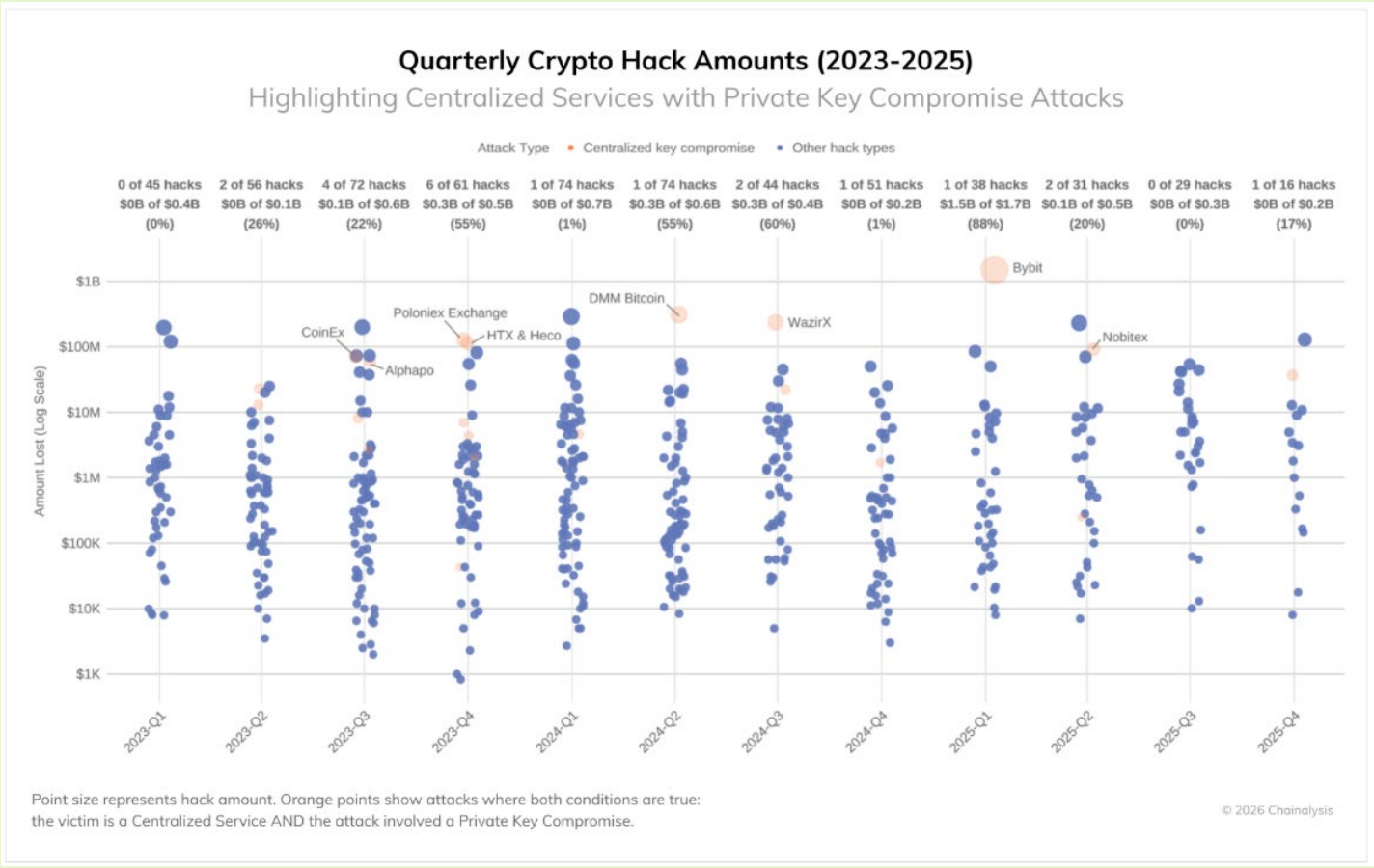
1. **合計損失金額の大部分（76%）を占めるのは「インフラストラクチャ攻撃」**によるもので、45件のインシデントで22億ドルの損失をもたらし、インシデントあたりの損失額は約4,850万ドルになる。このカテゴリには、署名鍵／シードフレーズ、ウォレットインフラ、特権アクセス、フロントエンド環境の侵害が含まれる。**主な攻撃パターンは、ソーシャルエンジニアリング、開発者環境への侵入、アクセス制御や出金ガバナンスの弱点を突いた運用環境の侵害（乗っ取り）**である
2. 「コードエクスプロイト」は件数的には最も多かった (52件) ものの、合計損失金額に占める割合は比較的小さく(3.5億ドル、12.1%)、インシデントあたり670万ドルであった
3. 損失金額の第3位である「プロトコル攻撃」（2億7,700万ドル、9.6%）は、発生件数こそ少ないものの（25件）、インシデントあたりの平均損失額は約1,110万ドルに上り、1件あたりの深刻度が高いことが分かる

参考：「2026 Crypto Crime Report – Illicit Crypto Trends & Typologies」（TRM Labs）_2026年2月時点

【一部の大規模インシデントへ被害が極端に集中する要因②】インフラストラクチャへの攻撃は、発生頻度が低いものの被害が甚大になりやすい

暗号資産被害に関する直近の動向（3/5）

- **中央集権的なサービスを標的とした、署名鍵インフラや署名プロセスに対する高度な攻撃**による被害額は全体の高い割合を占めており、**2025年第1四半期はBybit事案の影響で88%**に達した
- これらの攻撃は発生頻度こそ低いものの、ひとたび発生すると被害額が極めて甚大になるという特徴がある
- 標的とされたサービス提供者は、組織的なリソースと専門的なセキュリティチームを持つにもかかわらず、コールドウォレットの制御を回避するような高度な攻撃を完全に防ぎきれていないのが実情である。**攻撃者は、外部（サードパーティ）ウォレットとの連携機能を悪用し、正規の署名者を騙して悪意のあるトランザクションを承認させる手法**等を用いている
- 国家の支援を受けるハッカーグループが、IT技術者を装った人員をCEX、カストディアン、およびWeb3企業に潜入させ、特権アクセスを奪取する手口を近年の主要な攻撃手法として、影響の大きいインシデントを引き起こしている例も見られる



凡例（デロイトが補記）　中央集権的なサービスの署名鍵インフラ等に対する攻撃　その他攻撃

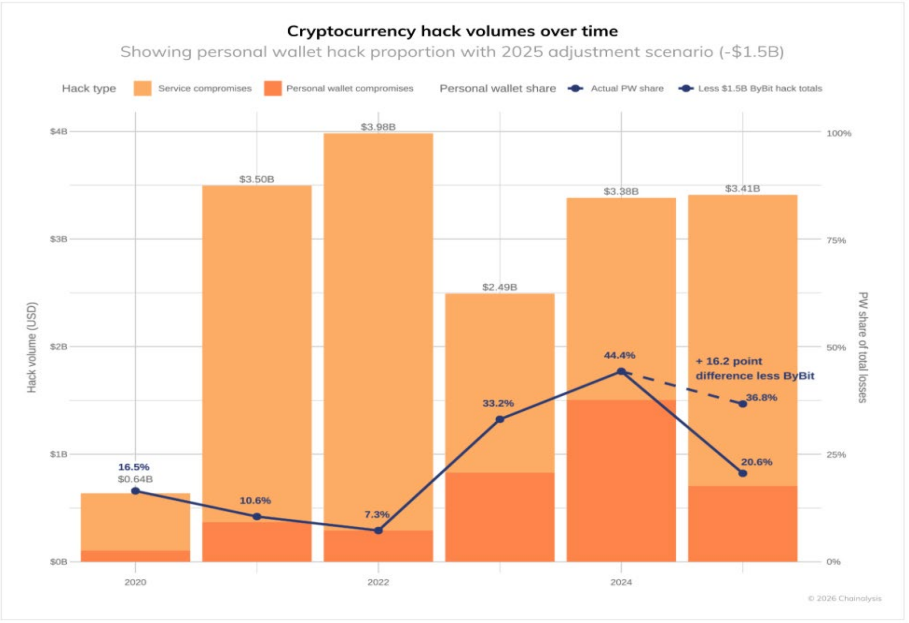
※丸のサイズは被害額の大きさを表す

参考：「2025 Crypto Theft Reaches $3.4 Billion」（Chainalysis）_2025年12月時点

【一部の大規模インシデントへ被害が極端に集中する要因③】近年においては、個人ウォレットを狙う攻撃の割合が急増し、被害規模の格差が拡大している

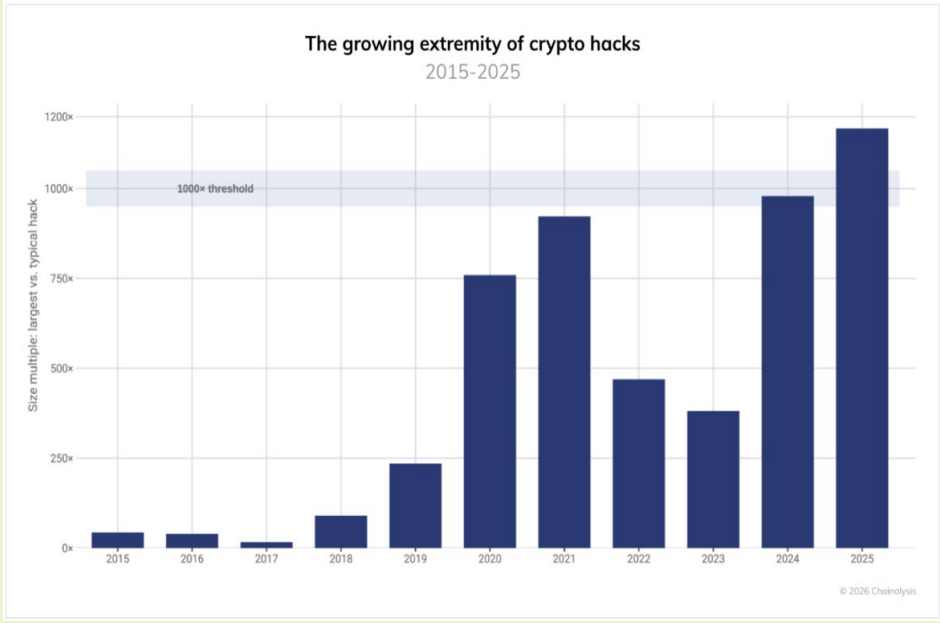
暗号資産被害に関する直近の動向（4/5）

- Chainalysis社の集計によると、2025年の暗号資産の盗難事件の被害額は34億ドルに上り、2月のBybit事案の被害 (15億ドル) だけでその総額の約半分を占めている
- 近年の盗難事件においては、「暗号資産サービスに対する攻撃」から「個人ウォレットに対する攻撃」へのシフトや、被害額における格差の拡大等の傾向がみられた



凡例（デロイトが補記）

- 暗号資産サービスに対する攻撃
- 個人ウォレットに対する攻撃



盗難事案を「暗号資産サービスに対する攻撃」と「個人ウォレットに対する攻撃」に分類すると、「個人ウォレットに対する攻撃」の割合の増加がみられる。2022年は7.3%であったが、2024年には44%、2025年には37%へ増加（2025年の数値は、極端な外れ値であるBybit事案の被害額を除外して算出）。

これまでも一部の大規模事件（外れ値）が被害額の大半を占める傾向にあったが、2025年は「最大被害額の事案」と「全事案の被害額の中央値」の差が初めて1,000倍を突破した。上位3件の大規模事案による被害額は、全体の約7割（69%）を占めている。**被害規模の格差が拡大**し、一部の事件に被害額が極端に集中していることが分かる。

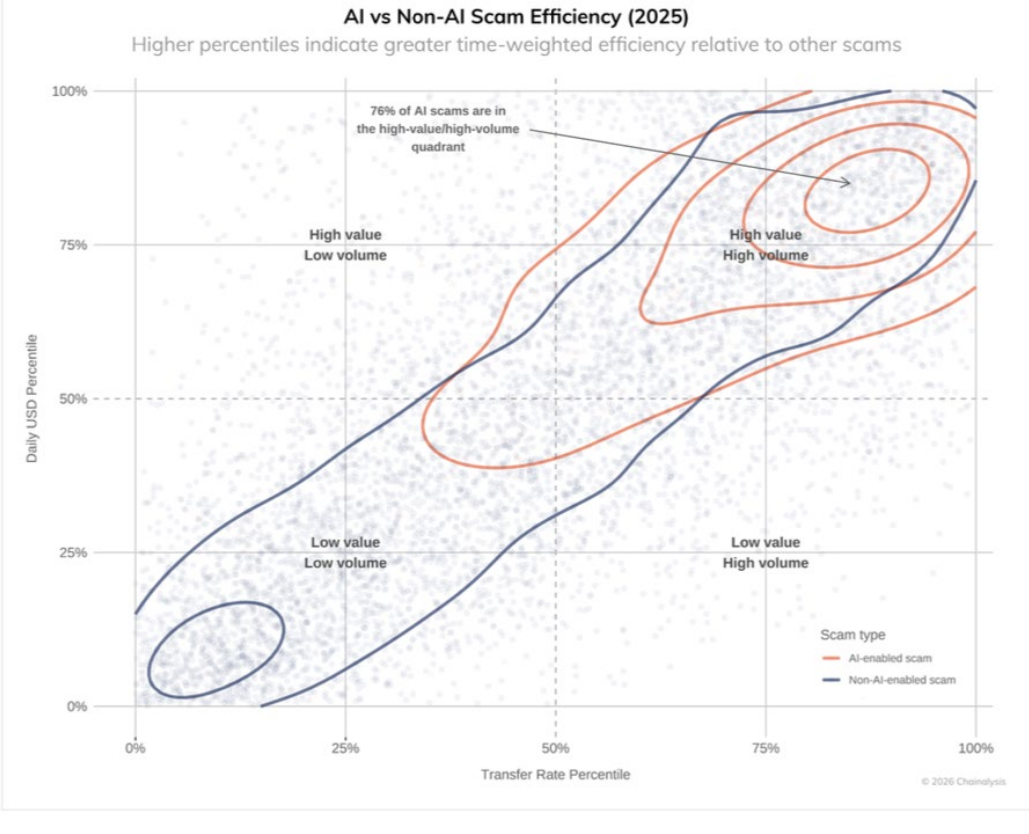
参考：「2025 Crypto Theft Reaches $3.4 Billion」（Chainalysis）_2025年12月時点

* 上記レポートは2026年1月以降の情報を含まないが、直近においては、DeFiを中心とした暗号資産サービスに対する攻撃が増加傾向にある。

詐欺の手法において、ディープフェイクや顔交換ソフトウェアを利用したAIの導入が急速に進んでいる

暗号資産被害に関する直近の動向（5/5）

- AIを利用しない詐欺の平均被害金額が約71万9,000ドルであるのに対し、AIを利用した詐欺では平均320万ドルが奪われており、1件あたりの被害金額が平均して4.5倍となっている
- 1日あたりの被害金額の中央値を見ても、通常の詐欺が518ドルであるのに対し、AI詐欺では4,838ドルと増加している
- また、国家が支援する脅威アクターが、暗号資産及びDeFi分野を標的として、被害者を欺くためにAI生成動画を使用するケースなども見られた



詐欺案件でAIが活用される傾向が顕著に見えており、「AIを利用しない詐欺」と「AIを利用する詐欺」を、被害金額（縦軸）、被害件数（横軸）でプロットして可視化すると、AIを利用しない詐欺（青色）に比べて**AIを利用した詐欺（オレンジ色）の方が被害金額、被害件数が多くなることが分かる。**

AI詐欺の1日あたりの平均送金回数は35.1回であり、非AI詐欺の3.89回に比べて**約9倍である。**

AIを利用した詐欺では、主にディープフェイク技術やAI生成コンテンツを駆使して、ロマンス詐欺や投資詐欺において極めて説得力のある「なりすまし」を行っている。
AIの導入は詐欺の「説得力」を高めるだけでなく、犯罪者が**より多くの被害者を同時に管理し、ターゲットにすることを可能にしていることが分かる。**

左図の縦軸は被害金額（Daily USD Percentile）、横軸は被害件数（Transfer Rate Percentile）を示している

凡例（デロイトが補記）
- AI Enabled Scam
- Non-AI Enabled Scam

参考：「The 2026 Crypto Crime Report - English - Chainalysis」（Chainalysis）_2026年3月時点
「UNC1069 Targets Cryptocurrency Sector with New Tooling and AI-Enabled Social Engineering」（Google Cloud）_2026年 2 月時点

1. 暗号資産関連のサイバー攻撃の発生状況とリスク評価
1.2 プレイヤー俯瞰とサイバーセキュリティ特性

ブロックチェーンは信頼の対象を再定義するものと期待されたが、実際の運用は従来型のモデルとの混合で行われているため、両者の特徴を踏まえた分析が必要である

中央集権型システムと分散型システムのサイバーセキュリティ特性比較

	理念としての違い		実世界での運用
	中央集権型システム（第三者依存）	自律分散型システム（プロトコル依存）	暗号資産事業での運用例（混合型）
信頼の対象	**第三者** 特定の管理主体がセキュリティを担保	**暗号学的証明** 数学的な正当性と分散合意が担保	**事業者への信用** 分散型資産の管理を、特定の事業者等に委ねるモデル
防御の考え方	**多層防御・ゼロトラスト** 預託資産を保護するため、認証・認可を厳格化し、侵入前提で監視	**自己主権型管理** 自身の署名鍵の安全管理が前提。オンチェーンで成立した取引の事後的な停止や取消は原則として困難	**重要資産の隔離** Web技術で防御しつつ、資産（署名鍵）はコールドウォレット等で隔離
権限管理	**IDプロバイダ依存** 管理者がリセット・停止可能	**署名鍵依存** 紛失＝資産喪失。誰も許可を出さない／止められない	**ID管理 ＋ 鍵の代理管理** ユーザーはID／PWを使うが、裏で事業者が署名鍵を管理
不変性 (Immutability)	**管理者が担保** 権限があれば書き換え可能	**事後修正困難性** 管理者が不正と考えられ得る取引であっても事後的な取消が困難	**二重帳簿の整合性確保** 社内DBとブロックチェーンの同期を事業者が担保
最大のリスク	**情報漏洩・権限濫用** データは改ざん・コピーされ得るが、原資産は残る場合が多い	**資産の不可逆的な喪失** 資産そのものが即時に移動し、取り戻せない	**単一障害点への攻撃集中** 中央集権的な防壁が破られ、分散型資産が盗まれる

実際起きていること

■ **発生している事象**

- ブロックチェーンは「信頼を置く場所を分散し、検証可能にできる部分を増やす技術」であり、完全な自律分散型システムの設計は難しい。その補完のために必要となる組織・運用が中央集権的で、その脆弱性に起因した巨額なハッキング事件が絶えない

■ **構造的課題**

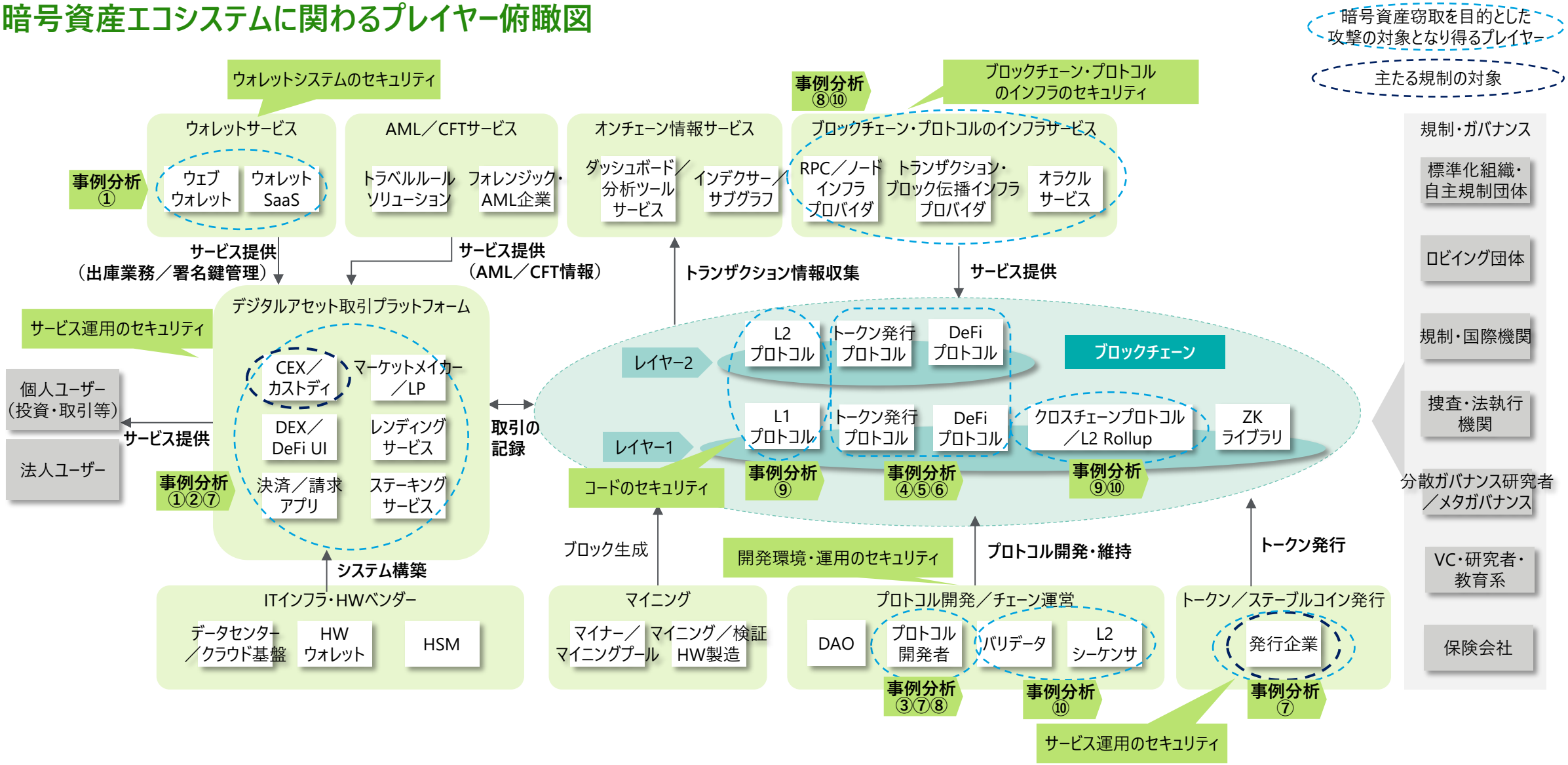
- **中央集権型と自律分散型の双方のリスクを併せ持つアーキテクチャ：**
  - **インターネット直結型の価値移転**
    高流動性資産がグローバルに公開ネットワークへ常時接続され、攻撃成功時の期待値が極めて高い構造となっている
  - **リスクの相互増幅**
    UI／API・鍵管理・ブリッジ等の中央集権的構成要素が単一障害点となる一方、インシデント発生後はオンチェーン確定により取引停止・巻き戻しが困難。中央集権の脆弱性と自律分散型の不可逆性を同時に抱える構造となっている
- **防御コストの構造的増大：**
  - **最高グレードの即時流出リスク**
    グローバル即時決済・匿名性・回収困難性により、攻撃成功時の損失規模が極端に大きい
  - **運用依存型セキュリティへの回帰**
    高度な鍵管理（MPC／HSM）、多層承認、常時監視、外部監査等によりリスクを補完する必要があり、防御コストは構造的に増大している

■ **本報告書の立場**

現実の運用は純粋分散モデルではなく、中央集権的要素と自律分散型基盤が混在する「複合アーキテクチャ」である。本報告書では、この構造的前提を踏まえ、オフチェーン要素・運用統制・ガバナンスを含む包括的なリスク評価を行う。

暗号資産エコシステムは多様なプレイヤーで構成され、直接の規制・監督対象外の主体も多い。エコシステム全体を俯瞰し、攻撃対象や影響を把握することが求められる

暗号資産エコシステムに関わるプレイヤー俯瞰図



学術論文および公的レポートのアプローチを参考にした上で※、システムの階層化および相互関連性の分析を進めることで、業界構造とリスクの所在を明らかにする

先行研究から得られた調査研究アプローチの示唆

先行研究
- 学術論文 -

暗号資産関連事業に関するサイバーセキュリティに係る学術論文では、自律分散型システムの技術特徴を以下のように整理する傾向がみられた

- ■ データの耐改ざん性と透明性
- ■ 分散的な実装方式と権限管理
- ■ 合意形成メカニズムの導入
- ■ スマートコントラクトの設計　等

従来と異なる技術的特徴を織り込んだシステムの階層モデルを再整理した上で、セキュリティに与える脅威や脆弱性を類型化し、
リスク要因の分析をするアプローチがみられた

先行研究
- 公的レポート -

公的機関・国際機関のレポート等では、上述同様に自律分散型システムの技術特徴を抽出し、システム的要素を踏まえながら、

- ■ 運用とガバナンスの構築および課題
- ■ 鍵管理・権限管理・ウォレット運用の重要性
- ■ 金融サービス提供に係るプレイヤーと市場ダイナミックス
- ■ 既存の規制・基準

等、技術面以外の観点からも分析している傾向がみられた

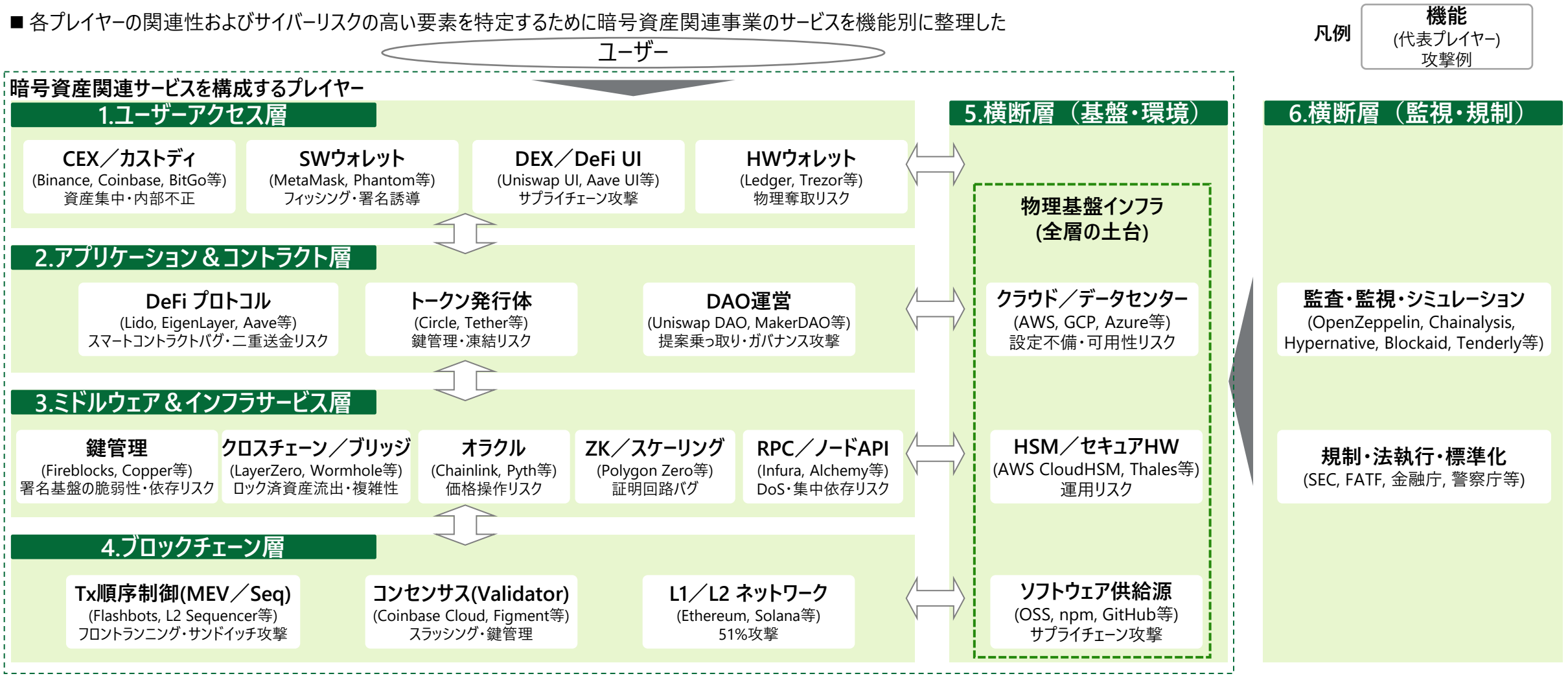
※Appendix1. 先行研究　参照

1. 暗号資産関連のサイバー攻撃の発生状況とリスク評価
1.3 サプライチェーンの機能別整理と攻撃手法

各事業者は、サプライチェーンにおける機能間の相互関連性を明らかにしたうえで、提供するサービスに影響を及ぼすリスクを分析することが必要である

暗号資産関連サービスを構成するプレイヤーの機能別整理

■ 各プレイヤーの関連性およびサイバーリスクの高い要素を特定するために暗号資産関連事業のサービスを機能別に整理した

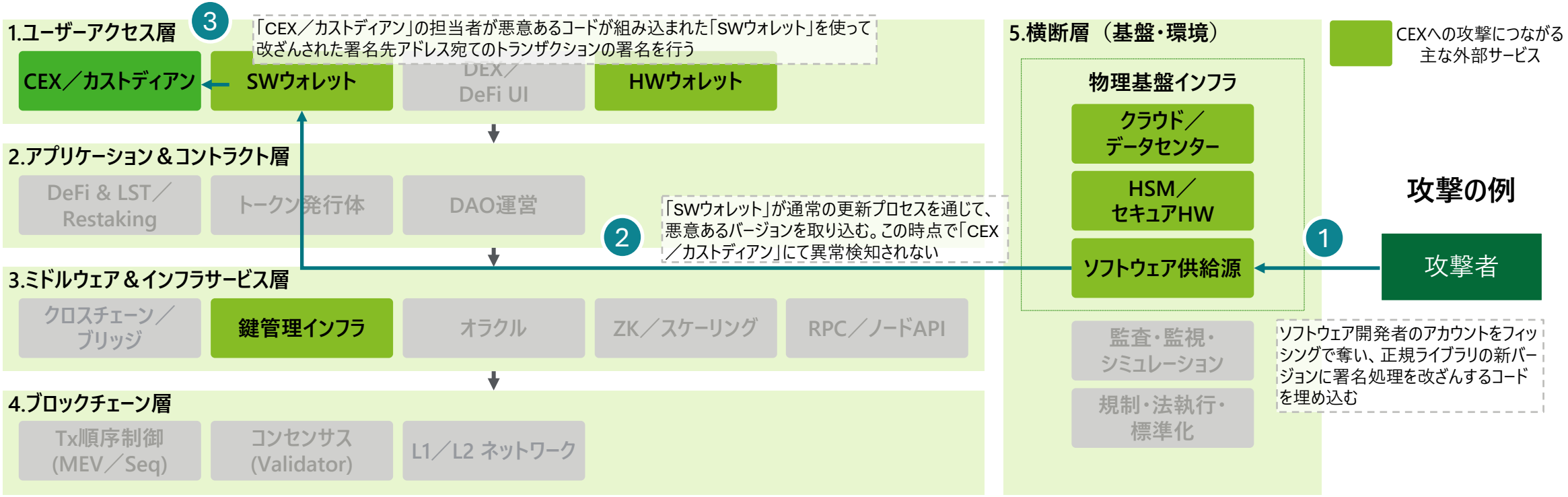


CEX運営における外部プレイヤーへの依存、とりわけ署名等の重要領域にかかるサービスの利用では、再委託先も含めたサプライチェーンを適切に管理していくことが推奨される

CEX運営において想定される統制範囲

■ **統制範囲の限界とサプライチェーン攻撃**
「CEX／カストディアン」が直接コントロールできるのは、自社が保有するインフラと従業員の権限・手続きに限られる。
一方、ウォレットSaaS、開発、監視基盤等外部サービスは、セキュリティ水準や運用が提供事業者の裁量に依存するため、「CEX／カストディアン」からの統制は、契約および一定のモニタリング等に基づく間接的なものにとどまる。特に鍵操作や署名プロセスに関与する外部サービスは、侵害時に資産流出へ直結し得る「致命点」となる

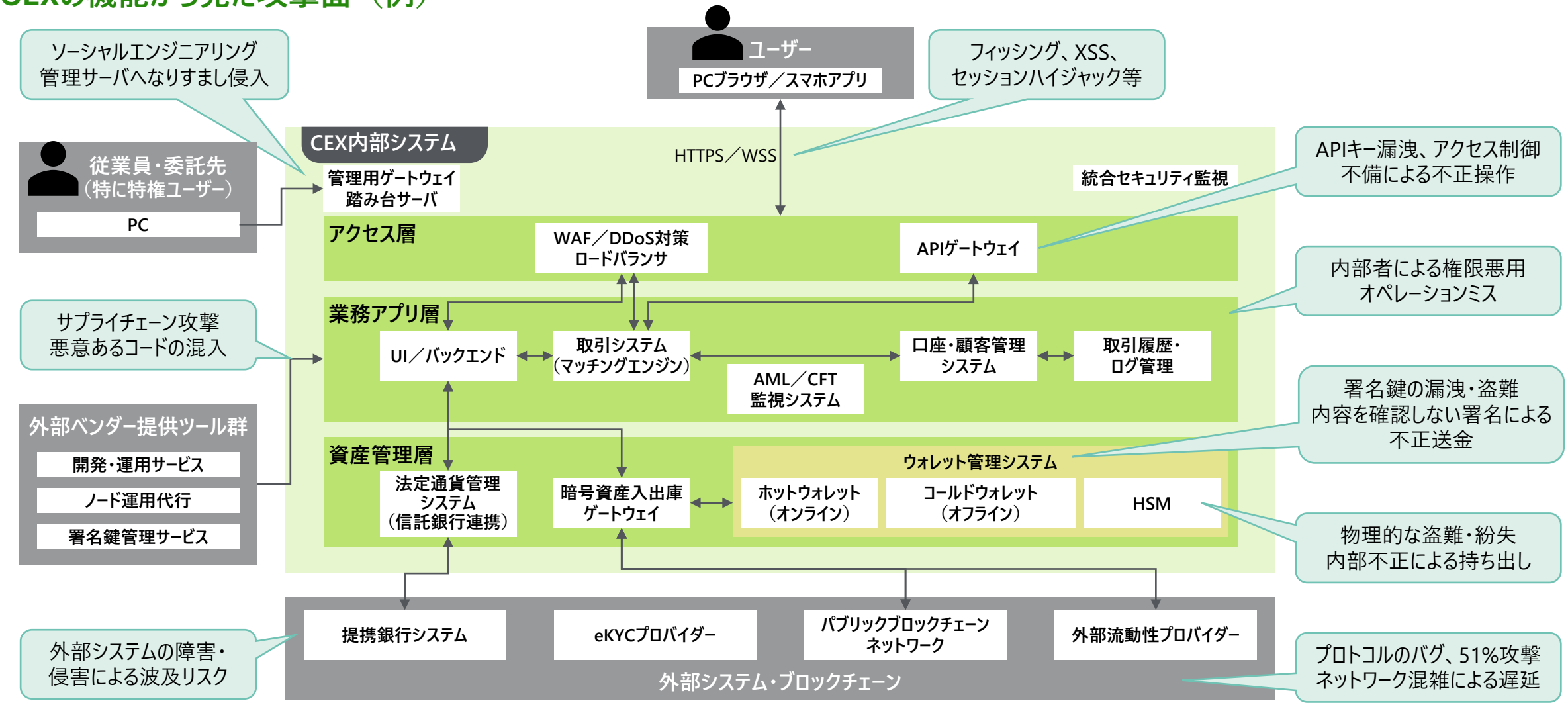
■ **再委託構造によるブラックボックス化**
「CEX／カストディアン」が委託する事業者は、さらにサブベンダーへの再委託を行っており、透明性の欠如が連鎖攻撃を発生させる。再委託先の確認や監督を適切に実施することの重要性が高まっているが、実務では追跡不能な多層委託が残り得る



注：本図は構成の一例であり、実際に利用する外部プレイヤーはCEX各社によって異なる可能性があることに留意

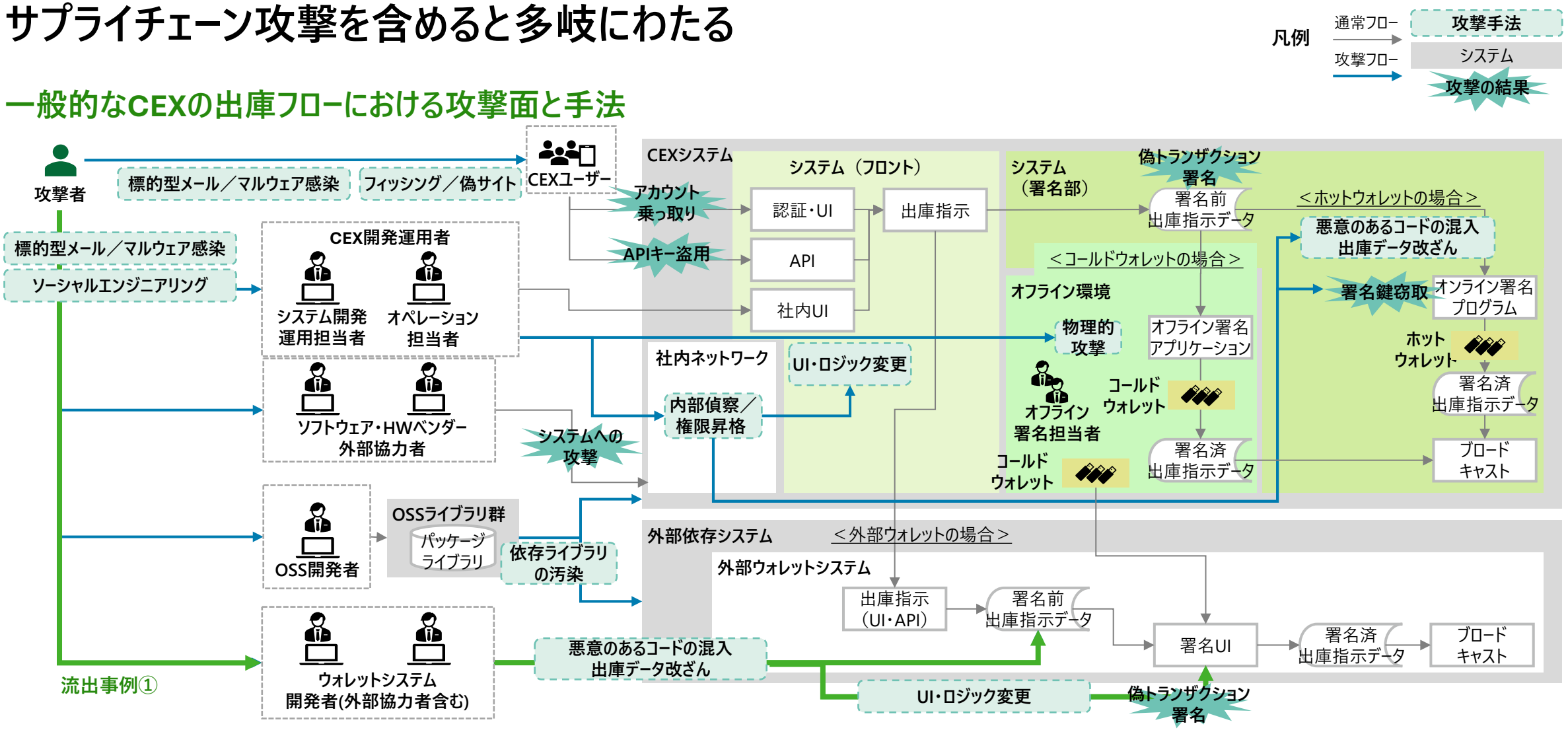
CEXのシステムに対して、攻撃者がどのチャネルからアクセスしてくる可能性があるかを明らかにして、適合する対応策を講じる必要がある

CEXの機能から見た攻撃面（例）



CEXに対する攻撃面と手法は、自社システムのみならず外部システムを通じたサプライチェーン攻撃を含めると多岐にわたる

一般的なCEXの出庫フローにおける攻撃面と手法



CEX開発運用者を経由する攻撃：CEX開発運用者へのソーシャルエンジニアリング等により社内ネットワークに侵入し、悪意のあるコードの混入、UI・ロジック変更、物理攻撃によってCEXシステムの中枢（出庫指示や署名等）を攻撃する手口
ソフトウェア・HWベンダー外部協力者を経由する攻撃：外部の開発協力者へのソーシャルエンジニアリング等により社内ネットワークに侵入し、悪意のあるコードの混入、UI・ロジック変更、物理攻撃によってCEXシステムの中枢を攻撃する手口
OSS（オープンソースソフトウェア）開発者を経由する攻撃：標的型メール等でOSS開発者を侵害し、OSSライブラリを汚染してCEXシステムまたは外部ウォレットシステム全体へ波及させる手口
（※OSS: コードが公開されているソフトウェア／ライブラリ: 他のシステムから部品として使われるプログラム）
ウォレットシステム開発者を経由する攻撃：ウォレットシステム開発者へのソーシャルエンジニアリング等によりPCにマルウェアを感染させて外部ウォレットシステムへの接続権限を取得し、悪意のあるコード混入、UI・ロジック変更によって外部ウォレットシステムの中枢を攻撃する手口

2. 近年の主要な流出インシデントの原因と対策の検討

2.1 事例分析対象の選定

暗号資産関連業者への攻撃は、フィッシング・マルウェア等の古典的手口から、スマートコントラクトやブロックチェーン関連ソフトウェアの脆弱性悪用まで多岐にわたる

暗号資産関連業者への攻撃手法の例

ソーシャルエンジニアリング・フィッシング

システムの脆弱性ではなく、人間の心理・不注意を悪用して認証情報や機密情報を取得する攻撃や、偽のメール・SMS等で利用者に本物と誤認させてID・パスワード等を入力させる攻撃

マルウェア攻撃

悪意のあるソフトウェア （マルウェア） を使用して暗号資産を盗み取る。

マルウェアには以下の種類がある：

- キーロガー：キーボード入力を捕捉して機密情報を記録できるソフトウェア
- フィッシング：前項のフィッシング活動で使用するソフトウェア
- RAT (Remote Access Trojan)：被害者のハードウェアを乗っ取り、ウォレットや機密情報にアクセスできるようにするソフトウェア
- クリプトジャッキング：暗号資産マイニングの目的で、ユーザーのPCをハイジャックしてコンピューティングリソースを乗っ取るソフトウェア

APIの侵害

開発者のPC、内部システム等を侵害して、資金引き出し、トランザクション署名、アカウント管理等の重要な機能を制御するAPI資格情報を窃取する。これらのキーを使用して、攻撃者はトランザクション管理システムを乗っ取り、承認ロジックの脆弱性を特定し、大規模な不正送金を実行する。

脆弱な認証システム

ユーザーが推測されやすいパスワードを設定したり、どのプラットフォームでも同一のパスワードを設定している場合、認証強度が低いため、犯罪者に突破され、ウォレット等にアクセスされ得る。

スマートコントラクトの脆弱性

スマートコントラクトの設計に内在する欠陥を悪用する。

例えば以下の攻撃例がある：

- リエントランシー攻撃：残高更新に関するスマートコントラクトの設計欠陥を悪用し、次の残高更新タイミングまでに、資金を引き出す関数を継続的に呼び出すことで、残高を超えた金額を引き出す
- アクセス制御の欠陥：アクセス許可のセキュリティ度が低いスマートコントラクトを悪用し、制限された関数を呼び出すことで、資金の移動や資産へのアクセス権を入手する
- ロジックのバグ：単純ではあるが頻繁に発生するコーディングエラーや見落とし（誤った条件設定、ロジックでの用語の定義不足等）により、当該スマートコントラクトの資金を使い果たす等のアクションを実行する

フラッシュローン攻撃

分散型金融（DeFi）プロトコルにおける、無担保融資（フラッシュローン）の仕組みを悪用した攻撃。攻撃者は、巨額の暗号資産を一時的に借り入れ、同じトランザクション内（瞬時）に市場価格を操作したり、スマートコントラクトの脆弱性を突くことで、不正に利益を得る。

例えば以下の攻撃手法がある：

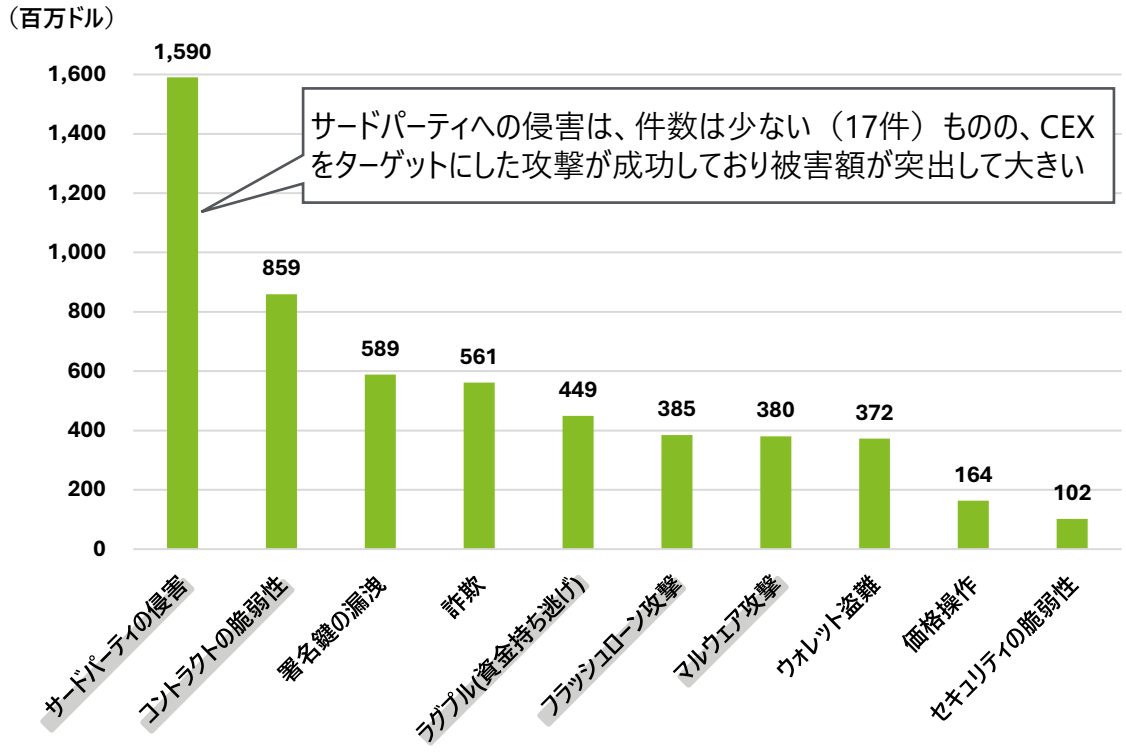
- 価格オラクル操作：特定のCEXで価格を操作し、その偽の価格を参考にして動いている別のレンディングプロトコルから、本来より安く資産を借りたり、不正に担保を清算させる
- 流動性プールの引き抜き：流動性プールから流動性を操作し、トークン価格を歪めて利益を得る
- ガバナンス攻撃：一時的に大量のガバナンス投票権を取得し、悪意のある提案を通過させて資金を奪う

参考 ：「Crypto Wallets Threat Intelligence Report」（NOMINIS）_2026年3月時点

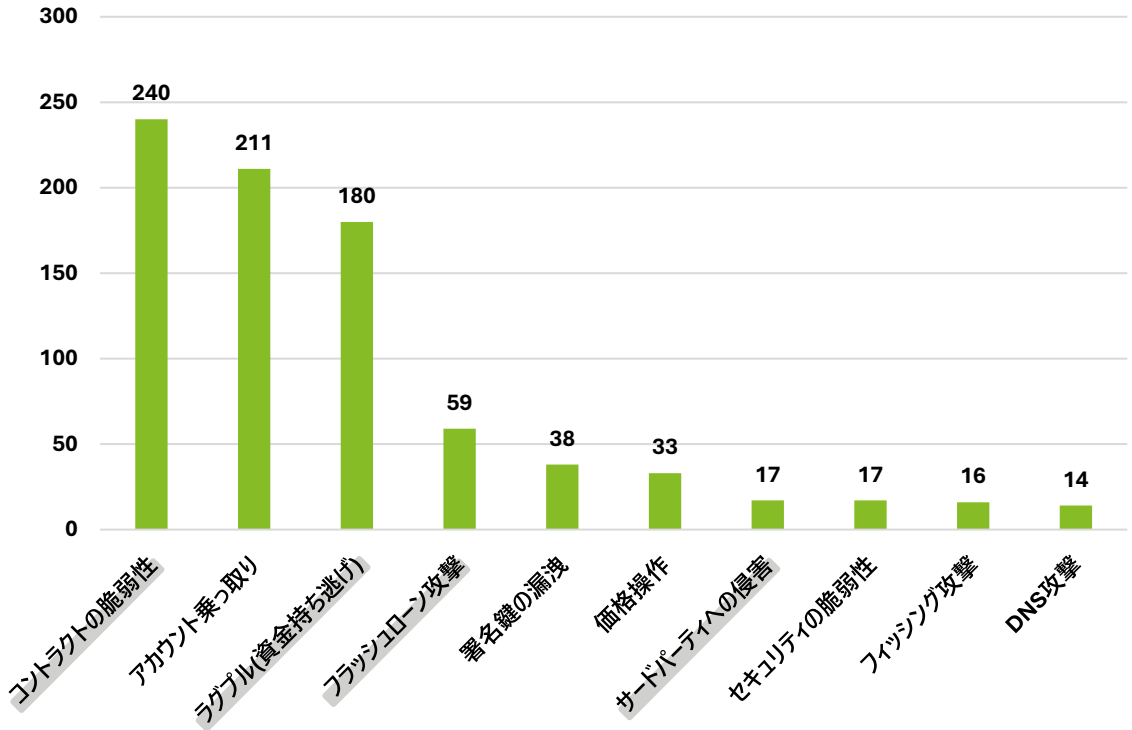
再掲

2023年以降は、サードパーティへの侵害を通じた攻撃や、スマートコントラクトの脆弱性を突いた攻撃の被害が顕著である

インシデント被害額順（2023年以降の累計）



インシデント件数順（2023年以降の累計）



参考：「SlowMist Hacked - SlowMist Zone」（SlowMist Hacked）_ 2023年1月~2026年1月21日の間発生した主なブロックチェーンハッキング事件の集計結果

- 被害額が大きい上位５つの攻撃手法について、次頁以降に被害額の大きな事例を記載
- 近年、DeFiプロトコルを狙ったインシデントが多数発生しており、そのうち特徴的な攻撃手法による事例を取り上げた
- 「署名鍵の漏洩」は、ゲーム・プラットフォーム会社の漏洩や、漏洩に関する攻撃手法の詳細が不明なケースが多いため、本資料では事例掲載を割愛した

被害額が大きい攻撃手法ごとに代表的事例を選定し、分析対象とした

攻撃手法別被害額の概要（被害額順、2023年1月～2026年1月）（1/2）

サードパーティへの侵害

	被害者	発生年月	被害額(M$)	概要
No.1	Bybit 事例分析①	2025年2月	1,460	サードパーティのウォレットサービス開発者へのフィッシング攻撃を起点に、事業者から資金が流出した。
No.2	Swiss Borg 事例分析②	2025年9月	42	暗号資産関連事業者において、サードパーティのステーキングサービスのエンジニアの認証情報が悪用され、ステーキングされていた資産が流出した。
No.3	BigONE	2025年7月	27	暗号資産関連事業者において、ホットウォレットの運用を制御するサードパーティ製ソフトウェアのロジックが改ざんされ、資産が流出した。
No.4	Fixed Float	2024年2月	26	暗号資産関連事業者において、ウォレットシステムを含む主要なサーバの権限を奪取されて資金が流出した。
No.5	Fortress	2023年9月	15	カストディアンにおいて、サードパーティの従業員がソーシャルエンジニアリング攻撃を受け、顧客アカウントが乗っ取られて資産が流出した。

スマートコントラクトの脆弱性

被害者	発生年月	被害額(M$)	概要
Cetus	2025年5月	230	DEXにおいて、最小限のトークン預入で流動性プールから大量の資産が引き出された。
Balancer v2 事例分析④	2025年11月	121	スマートコントラクトの丸め誤差等を利用してトークン価格を操作し、過小評価されたトークンを入手・交換して大量の資金を得た。
GMX	2025年7月	42	DEXにおいて、トークン価格を人為的に操作された後に換金され、資産が流出した。
Penpie	2024年9月	27	DeFiプロトコルにおいて、悪意あるコントラクトが作成され、多額のステーキング報酬が流出した。
Thala	2024年11月	26	DeFiプロトコルにおいて、アカウントのトークン残高不足にも関わらず流動性プールから多額の資産が引き出された。

ラグプル（資産持ち逃げ）

被害者	発生年月	被害額(M$)	概要
LIBRA	2025年2月	250	アルゼンチン大統領の宣伝によりトークン価格が急騰したがその後暴落、多くのウォレットが損失を抱えた。
Zkasino	2024年4月	33	賭博プラットフォームにおいて、顧客の担保トークンの返金が拒否され、プラットフォーマーが外部に担保トークンを移動した。
BALD	2023年7月	26	Layer2ネットワーク上で、ミームコイン発行者が価格が急騰した時点で大量のトークンを引き出した。
IBX trade	2024年10月	22	プロジェクトの資金調達において、ユーザー資金がプロジェクト主催者のアドレスに送金された。
Essence Finance	2024年10月	20	ステーブルコインプロジェクトにおいて、大量の担保トークンが引き出された直後に価格が暴落した。
Kokomo Finance 事例分析⑥	2023年3月	4	主催者がコントラクトを悪意のあるコードへ差し替えて、外部のアドレスにユーザー資産を転送し持ち逃げした。

注：攻撃手法の用語（Third-Party Vulnerability, Contract Vulnerabilityなど）は出典元の表記を引用している
注：複数の攻撃カテゴリーに跨る攻撃も存在する
参考：「https://hacked.slowmist.io/en/」（SlowMist Hacked）_ 2026年1月時点

被害額が大きい攻撃手法ごとに代表的事例を選定し、分析対象とした

攻撃手法別被害額の概要（被害額順、2023年1月～2026年1月）（2/2）

フラッシュローン攻撃

	被害者	発生年月	被害額(M$)	概要
No.1	Euler Finance 事例分析⑤	2023年3月	197	攻撃者は上限なく担保トークンの寄付ができるスマートコントラクトの脆弱性を突いて意図的に強制清算を引き起こすと同時に、清算人に成りすますことで多額の報酬を得た。
No.2	Hedgey	2024年4月	45	攻撃者はフラッシュローンを使用したスマートコントラクトの脆弱性攻撃によりEthereumとアービトラムネットワークの２つのチェーンから資金を流出させた。
No.3	Sonne Finance	2024年5月	20	Compound v2のフォークに見られる既知の脆弱性（Precision Loss）を突き、必要な量よりも少ない担保トークンを返却することで、より多くの原資産を引き出すことに成功。
No.4	Polter Finance	2024年11月	12	プロトコルには価格オラクル操作の脆弱性があり、攻撃者はフラッシュローンを借りた後で、トークンの認識価格を変更し、水増しされた担保で借り入れと返済を行い、差額を窃取。
No.5	Platypus	2023年2月	9	プロトコルのステーブルコイン支払い能力チェック機能の脆弱性により、攻撃者はフラッシュローンの借入を担保として借り入れ、その後、債務を支払わずに引き出すことができた。

マルウェア攻撃

被害者	発生年月	被害額(M$)	概要
Radiant Capital 事例分析③	2024年10月	50	開発者がPDFを偽装したマルウェアに感染し、感染PC上でトランザクションが改ざんされ、資金が流出した。
Poly Network	2023年7月	10	攻撃者は盗まれた署名鍵を用いて、偽のブロックヘッダーと検証署名を生成し、検証プロセスを回避して資金を流出させた。プログラムのコンパイル環境にマルウェアが仕込まれ、バリデータノードの署名鍵が盗まれた可能性がある。
Truflation	2024年6月	6	攻撃者はマルウェア攻撃によりシステムに侵入してウォレットの複数の署名鍵を収集し、偽のトランザクションに署名し資金を流出させた。
Tapioca DAO	2024年10月	5	開発者がマルウェアに感染して署名鍵が漏洩し、その鍵を使ってトークン権利確定コントラクトが乗っ取られた。これにより、コントラクト内のトークンを窃取した。
CoinStats	2024年6月	2	従業員がソーシャルエンジニアリングによって社内コンピュータにマルウェアをダウンロードさせられ、そこからAWSインフラにアクセスされたことで、署名鍵を窃取して資金を流出させた。

注：複数の攻撃カテゴリーに跨る攻撃も存在する
参考：「https://hacked.slowmist.io/en/」（SlowMist Hacked）_ 2026年1月時点

2026年２月以降の事例についても、DeFiをはじめとする暗号資産サービスに対する攻撃を分析対象とした

2026年２月以降の代表的事例

■ DeFiサービスへの攻撃においても運用の脆弱性を突く攻撃が見られ、CEXにおける脅威・脆弱性を検討するにあたって参考となる事例が多い
■ ブロックチェーンのノード処理不備により発生するReorgを利用した攻撃やノードインフラへの攻撃など、ウォレットに限定されないサプライチェーンのリスクが顕在化している

被害者	発生年月	被害額(M$)	攻撃手法	概要
Resolv Protocol 事例分析⑦	2026年3月	25	ソーシャルエンジニアリング＋ガバナンスの脆弱性	外部協力者のGitHub資格情報を起点にリポジトリへ侵入して認証情報を窃取。その後クラウド環境に侵入し、ポリシーを変更することで署名権限を奪取し、不正にトークン（USR）を大量ミント
Drift 事例分析⑧	2026年4月	285	ソーシャルエンジニアリング+ガバナンスの脆弱性	ソーシャルエンジニアリングによりdurable nonce（署名トランザクションを後日実行できる仕組み）を使って事前署名を取得し、admin権限を奪取。偽トークンを担保としてUSDC・SOL等の実資産を不正に引出
Litecoin 事例分析⑨	2026年4月	0.6	ブロックチェーンのreorgを利用した攻撃	MWEBの検証不備とノード処理不備により発生した13ブロックのチェーン再編成（reorg）を利用。Litecoinチェーン側の入金は取り消されたが、Bitcoinチェーン側で残存した資産を不正に持ち逃げ。
Kelp DAO/ LayerZero 事例分析⑩	2026年4月	293	基盤インフラへの攻撃	ノードインフラへの攻撃とDDoS攻撃でLayerZeroブリッジ（OFT）の検証プロセスを悪用し、裏付けのないrsETH（約11.6万枚）を不正ミント。これを担保にDeFiで借入・換金することにより、資金が流出

参考：「https://hacked.slowmist.io/en/」（SlowMist Hacked）_ 2026年5月時点
参考：「https://neuralwired.com/2026/04/26/litecoin-mweb-zero-day-13-block-reorg/」（Litecoin 13-Block Reorg: MWEB Zero-Day Exploit Explained 2026）_2026年4月時点

2. 近年の主要な流出インシデントの原因と対策の検討
2.2 事例分析

本事案は、委託先の開発環境の侵害を起点に、UIを偽装して正規の署名プロセスを実行させ、資金流出が成立した攻撃である

Bybit事案の概要

■ 攻撃者は、Bybitが利用していた外部ウォレットサービス（Safe）に対してソーシャルエンジニアリングを仕掛け、トランザクション生成のためのUIを改ざんした。Bybitの担当者は、改ざんされたUIを用いて不正なトランザクションの生成を承認してしまった。署名に用いるハードウェアウォレット上では、不正なトランザクションの内容が表示されていたが、Bybitの署名者は、十分に確認しないまま署名してしまい、不正なトランザクションが実行された。その結果、ウォレットの管理権限が攻撃者に移され、資金流出につながった。

攻撃のタイムライン

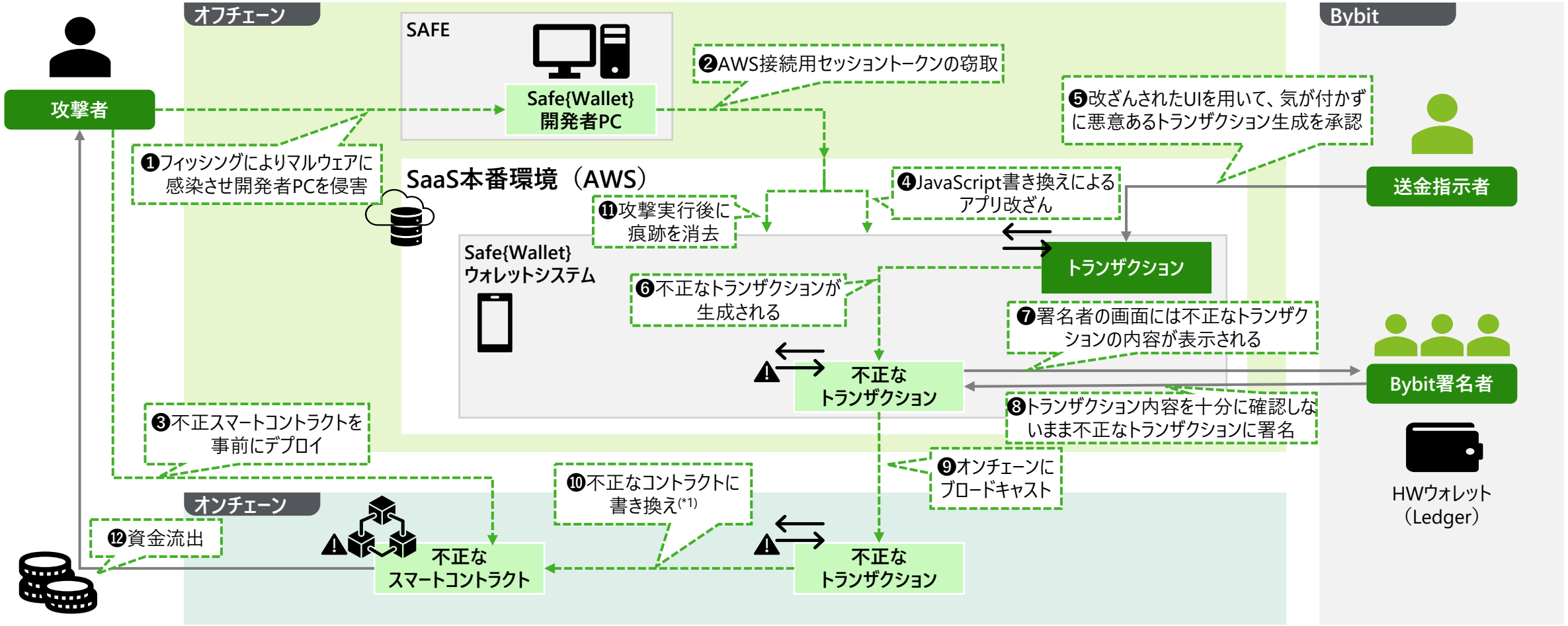
	No.	発生日時	主体	説明
初期侵入	❶ ❷	2025年2月4日～ (UTC)	攻撃者	フィッシングにより、**ウォレットベンダーの開発者PCをマルウェアに感染させ侵害**。AWSアクセストークンが不正に利用され始めた
	❸	2025年2月18日 15:39(UTC)	攻撃者	攻撃者は、**悪意のあるコントラクトをデプロイ**。このコントラクトは不正なトランザクションからコールされ、 引き出し機能を実装したコントラクトを呼び出す内容となっていた
	❸	2025年2月18日 18:00(UTC)	攻撃者	攻撃者は**引き出し機能を実装した別の悪意のあるコントラクト**をデプロイ
	❹	2025年2月19日 15:29(UTC)	攻撃者	悪意のあるコードを用いて、Safe{Wallet} のAWS S3 に格納されている**JavaScript ファイルを不正に変更**
トランザクション改ざん・署名誘導	❺ ❻	2025年2月21日 13:30(UTC)	Bybit	Bybitが Safe{Wallet} 経由で開始したトランザクションを**悪意のあるJavaScript ファイル**によって改変
	❼ ❽	2025年2月21日 14:11(UTC)	Bybit	Bybit の全署名者は、**侵害された Safe{Wallet} のUI経由で、悪意のあるトランザクションに署名** 侵害されたUIでは、トランザクションの正しい内容の詳細を表示しつつ、不正なトランザクションをHWウォレットに送信
	❾ ❿	2025年2月21日 14:13(UTC)	Bybit	署名済みの不正なトランザクションがEthereumブロックチェーンにブロードキャストされ、Bybitの**コールドウォレットのコントラクトをアップグレード**して、 資金を流出させるコントラクトのバックドア関数sweepETH()とsweepERC20()を実行
隠蔽・資金流出	⓫	2025年2月21日 14:15(UTC)	攻撃者	攻撃実行から2分後に、攻撃者はSafe{Wallet} AWS S3上のJavaScriptファイルを元の無害なファイルに復元し、**痕跡を消去して侵害を隠蔽**
	⓬	2025年2月21日 14:16(UTC)	Bybit	バックドアが埋め込まれたスマートコントラクトを介して、**コールドウォレットのすべての暗号資産が流出**

参考：「Bybit Incident Investigation Preliminary Report」（Verichains）_2026年1月時点

※各事例に関して公表されている資料及び本報告書の執筆時点で入手可能な情報に基づき調査研究の目的から整理したもので、個別事案に関する責任の所在又は法的評価を示すものではありません

本事案は、委託先の開発環境の侵害を起点に、UIを偽装して正規の署名プロセスを実行させ、資金流出が成立した攻撃である

Bybit事案における攻撃の全体像：オフチェーン侵害からオンチェーン資金流出まで



(*1): 2つのスマートコントラクトから構成されており、攻撃者はプロキシコントラクトから呼び出す実装コントラクトを自身が作成した不正なコントラクトに差し替えることで、暗号資産を窃取した
- プロキシコントラクト：記憶領域に実装コントラクトのアドレスを格納し、実行命令を受けると実装コントラクトを呼び出す
- 実装コントラクト（MasterCopy）：マルチシグ等のルールを定義している。デリゲートコール機能（外部のコントラクトに処理を委任する）を持つ

※各事例に関して公表されている資料及び本報告書の執筆時点で入手可能な情報に基づき調査研究の目的から整理したもので、個別事案に関する責任の所在又は法的評価を示すものではありません

本事案は、委託先の開発環境の侵害を起点に、UIを偽装して正規の署名プロセスを実行させ、資金流出が成立した攻撃である

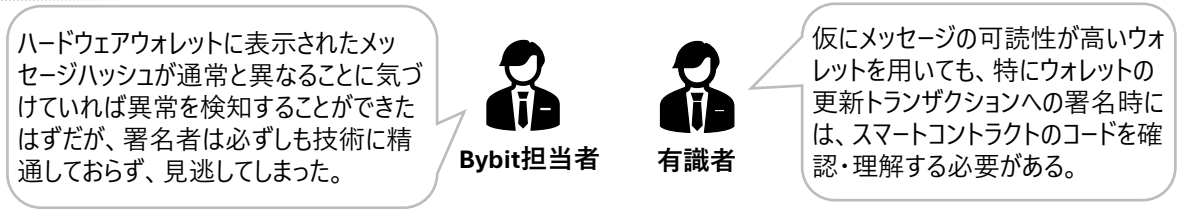
主要な事実関係と考えられる脆弱性・対策（1/2）

	事実	インシデントにつながった脆弱性	実施すべきだった対策	参考：MITRE ATT&CKの攻撃技法	参考：MITRE AADAPTの攻撃技法	参考：MITRE D3FENDの防御技法
SAFE	■ 暗号資産関連事業のウォレットアプリケーション（JavaScript等、AWS／S3バケットにホスト）を提供 ■ AWS環境の認証情報は開発者の端末に保存					
攻撃者	■ フィッシングにより開発者端末への侵入後、AWS環境へ接続するための有効なセッショントークンを窃取し、AWS環境へアクセスした	フィッシング対策が不十分	■ フィッシング対策の教育・（疑似）訓練	フィッシング (T1566)	アカウント取得 (ADT3001)	メッセージ分析 (D3-MA) ユーザー行動分析 (D3-UBA)
		本番環境認証情報の端末保存、認証情報管理が不十分	■ 短命認証、MFA、端末への長期認証情報保存禁止、認証情報ローテーション	アプリアクセストークンの窃取(T1528) アプリアクセストークンの利用(T1550.001)	サプライチェーン侵害 (ADT1195) 外部サービスの悪用 (ADT3008)	クレデンシャル強化 (D3-CH) 資格情報ローテーション (D3-CRO)
		クラウドアクセス制御、異常検知が不十分	■ 条件付きアクセス、JITアクセス、IP・端末制限、操作ログ監視	クラウドアカウント (T1078.004) サプライチェーン侵害 (T1195)	外部サービスの悪用 (ADT3008) サプライチェーン侵害 (ADT1195)	アクセス制限 (D3-AMED) リソースアクセスパターン分析(D3-RAPA)
	■ 署名者が利用するJavaScriptを不正なスクリプトへ差し替えた ① 特定の条件下（Bybitが関与する取引等）でのみ動作 ② トランザクションをスマートコントラクトの不正なアップグレードに改ざん ③ ウォレットのUIを偽装し、署名者に正当な取引であるように見せかける ④ 署名完了後、正当なトランザクションへ置き換え	未承認のプログラム変更の抑止・検知する統制が不十分 不正ロジックの検出が不十分 未署名トランザクションの改ざん防止・検知が不十分 署名確認プロセスが不十分	■ CI/CD統制、コード署名、変更承認、ホスト資産の完全性監視 ■ 本番コード差分監視、署名前のTxデコード、署名対象ハッシュ照合、コンテキスト検証 ■ 独立端末での検証、署名内容の二経路確認	送信データ改ざん (T1565.002) 偽装 (T1036)	スマートコントラクト実装の悪用(ADT3012) ブラインド署名 (ADT3012.006相当)	ファイル完全性監視 (D3-FIM) ファイル分析 (D3-FA) 取引コンテキスト検証 (D3-TV)

本事案は、委託先の開発環境の侵害を起点に、UIを偽装して正規の署名プロセスを実行させ、資金流出が成立した攻撃である

主要な事実関係と考えられる脆弱性・対策（2/2）

	事実	インシデントにつながった脆弱性	実施すべきだった対策	参考：MITRE ATT&CKの攻撃技法	参考：MITRE AADAPTの攻撃技法	参考：MITRE D3FENDの防御技法
Bybit	■ HWウォレット（Ledger）で署名。HWウォレット上、内容を容易に確認できる形式で表示されておらず、担当者は不正に気付けなかった ■ その結果、不正なスマートコントラクトのアップグレードがブロードキャスト ① 攻撃者コントラクト：全署名者が不正なトランザクションを承認するとデリゲートコールによって呼び出され、実装コードの宛先を②のアドレスへ書き換える ② バックドアコントラクト(Attacker's New Implementation)：大量の暗号資産を流出させる関数が組み込まれ、資金を窃取する	ブラインド署名(*1) 送金権限とアップグレード権限の未分離 更新可能コントラクトの管理統制不足 同一ウォレットでの資産集中管理、自動停止機能不足	■ メッセージの可読性が高いウォレット機能の導入 ■ サイバー攻撃を想定した署名担当者の教育・研修 ■ 送金権限とアップグレード権限の分離、複数者承認 ■ 複数ウォレットへの資産分散、出金上限、異常流出検知、サーキットブレーカー	送信データ改ざん (T1565.002) ユーザーによる実行 (T1204)	ブラインド署名 (ADT3012.006相当) コントラクトの所有権変更(ADT3012.001) 悪意あるコントラクト (ADT3012.002)	ファイル完全性監視 (D3-FIM) 取引コンテキスト検証 (D3-TV) 構成権限制御 (D3-SCP) アクセス制御 (D3-AMED)
攻撃者	■ 窃取した資金を複数のアドレスへ分割、またはチェーンホッピングで他のチェーンに移動しながら資金の追跡を困難にした				クロスチェーンスワップ(*2) (ADT3005) 資金の吸い上げ (ADT3028) レイヤリング(*3) (ADT3028.003)	

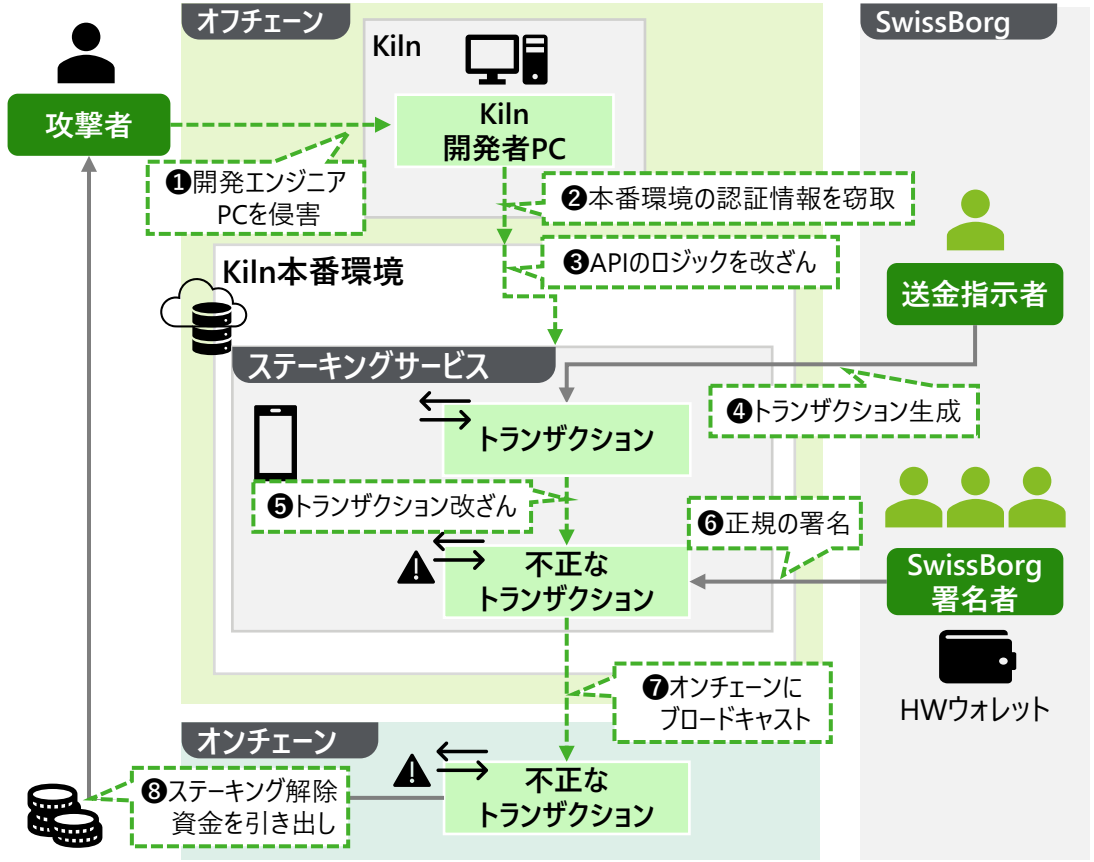


(*1): スマートコントラクトを含む複雑なトランザクション等に対して、ユーザーが署名内容の全容を画面上で確認できずに署名すること（P65参照）
(*2): 暗号資産を複数の異なるブロックチェーン間で取引し、出所を隠蔽する
(*3): 大量の暗号資産を小さな取引に分割し、様々なアカウントやウォレット、プラットフォームを通じて移動させることで追跡を困難にする

本事案は、サードパーティが提供するステーキングサービスのAPI改ざんにより、ステーキングのため預け入れていた資産が窃取された事例である

SwissBorg事案 全体像およびタイムライン

- 複数のCEX・DEXに同時接続して運用機能を提供するSwissBorg社は、ステーキングプラットフォームを提供しているKiln社のサービスに暗号資産を預け入れ、ステーキングを行っていた
- 攻撃者は、外部ウォレットサービスへの不正アクセス・プログラム改ざんによってトランザクションを改ざんし、SwissBorg社に気づかせずステーキングの引出権限を奪取し、ステーキング中の暗号資産を窃取した



攻撃のタイムライン

	No.	発生日時	主体	説明
初期侵入	❶ ❷	不明	攻撃者	Kilnのインフラエンジニアの GitHub アクセストークンを侵害して（手法は不明）、**本番環境システムにアクセス可能な認証情報を窃取。**
トランザクション改ざん・署名誘導	❸ ❺	不明	攻撃者	本番環境のKiln **APIエンドポイントのロジックを改変**して、正規のステーク解除トランザクションに加えて、悪意のあるトランザクションを返すように改ざん。
	❹ ❻ ❼	2025年8月31日 09:55(UTC)	SwissBorg	改ざんされたトランザクションを**デコードして確認することなく署名。**
資金流出	❽	2025年9月8日 12:02(UTC)	攻撃者	改ざんされたトランザクションにより、攻撃者はステーキング用口座の引出権限を得て、その後、資金のステーキング解除と引出を実行。

参考：「SwissBorg's $41M Exploit (Detailed Breakdown)」（QuillAudits）2026年3月時点

本事案は、サードパーティが提供するステーキングサービスのAPI改ざんにより、ステーキングのため預け入れていた資産が窃取された事例である

主要な事実関係と考えられる脆弱性・対策

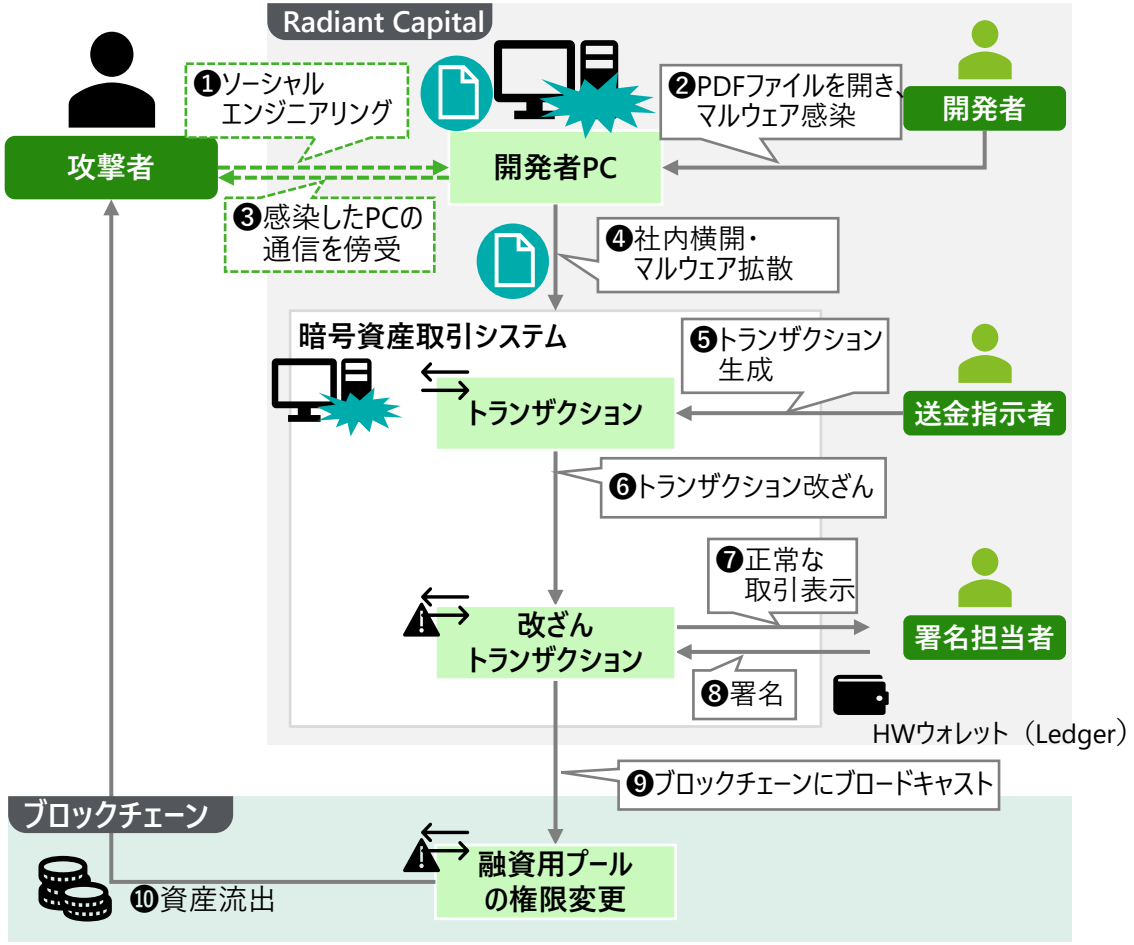
	事実	インシデントにつながった脆弱性	実施すべきだった対策	参考：MITRE ATT&CKの攻撃技法	参考：MITRE AADAPTの攻撃技法	参考：MITRE D3FENDの防御技法
Swiss Borg	SwissBorg社は暗号資産投資プラットフォームを営んでおり、ステーキングサービスの提供のため、ステーキングプラットフォームを提供しているKiln社のサービスを利用していた	GitHubトークン管理・MFA・失効管理が不十分 本番環境認証情報の厳格な管理不足 API変更管理・本番反映統制が不十分 APIレスポンス検証不足 Tx内容確認不足 条件付き不正ロジック検知不足	■ 本番環境の認証情報の厳格管理、短命化・ローテーション ■ 変更承認・API完全性監視、APIレスポンス検証、Txデコード ■ APIレスポンスの検証・チェック ■ 権限変更イベント監視、閾値監視	アプリアクセストークンの窃取(T1528) 有効なアカウント(T1078) 保護されていない認証情報(T1552) 送信データ改ざん(T1565.002) イベントトリガー実行(T1546) サプライチェーン侵害(T1195)	アカウント取得(ADT3001) 外部サービス利用(ADT3008) スマートコントラクト実装の悪用(ADT3012) スマートコントラクトの所有権変更(ADT3012.001) サプライチェーン侵害(ADT1195)	クレデンシャルの強化(D3-CH) 多要素認証(D3-MFA) 資格情報ローテーション(D3-CRO) アクセス制御(D3-AMED) ファイル完全性監視(D3-FIM) アプリケーションの強化(D3-AH) 取引コンテキスト検証(D3-TV) ドメインロジック検証(D3-DLV)
Kiln	ステーキングプラットフォームを提供しており、セキュリティ面では第三者保証やスマートコントラクト監査を受けていた(*1)					
攻撃者	① 攻撃者は、何らかの方法によってKilnのインフラエンジニアのGitHubアクセストークンを侵害し、さらに、本番環境システムにアクセス可能な認証情報を窃取した ② 攻撃者は、本番環境のKiln APIエンドポイントのロジックを改ざんして、正規のステーク解除トランザクションに、悪意のあるトランザクションを付加するようにした。この悪意のあるトランザクションは、残高が一定額以上ある場合のみ、出金権限を変更した					
Swiss Borg	SwissBorgの署名者は、改ざんされたAPIから受信したトランザクションをデコードして内容を確認することなく署名し、実行した。(*2) その結果、攻撃者はステーキング用口座の引出権限を入手した	ブラインド署名(*3) 送金とアクセス権変更の権限未分離 同一ウォレットでの資産集中管理	■ メッセージの可読性が高いウォレット機能の導入、署名前デコード ■ スマートコントラクト権限の細分化と高権限の厳格な管理 ■ 複数のウォレットへの資産分散、出金制限	ユーザーによる実行(T1204) データ改ざん(T1565)	ブラインド署名(ADT3012.006相当)	取引コンテキスト検証(D3-TV) コンテンツ検証(D3-CV)
攻撃者	攻撃者は、ステーキング解除と引出を実行し、暗号資産を窃取した					

(*1): 本研究調査ではこれらの外部評価結果を入手していないため、評価の対象範囲や手法、検出された問題点の有無等の確認には至っていない
(*2): トランザクションの内容をデコード（内容解析）せずに署名する手法である。内容を検証せずに署名するためリスクが高く推奨されない。主に特殊なトランザクションや高度なDeFi操作で、署名を付加する際等に使われる
(*3): スマートコントラクトを含む複雑なトランザクション等に対して、ユーザーが署名内容の全容を画面上で確認できずに署名すること（P65参照）

本事案は、開発者へのソーシャルエンジニアリングと マルウェアによる攻撃を通じてトランザクションが改ざんされ、資金が窃取された事例である

Radiant Capital事案 全体像およびタイムライン

- Radiant Capital社（以下、Radiant）は、分散型クロスチェーンを利用した融資（DeFi）を提供していた
- 攻撃者は、開発者が感染したマルウェアを通じてシステムに侵入し、トランザクションを改ざんし、Radiant Capitalに気づかせないまま電子署名を行わせ、暗号資産を窃取した



攻撃のタイムライン

No.	発生日時	主体	攻撃のタイムラインの説明
侵入とマルウェア感染 ❶	2024年9月11日	攻撃者	同社の元の外部委託者を偽装してTelegramで連絡。PDFファイルに偽装したマルウェア実行ファイルを送付
侵入とマルウェア感染 ❷	2024年9月11日	Radiant	開発者がPDFファイルを開くと同時にマルウェアによりバックドアが設定、開発者PCが感染した
侵入とマルウェア感染 ❸	2024年9月11日	攻撃者	感染したPCの通信を傍受
侵入とマルウェア感染 ❹	2024年9月11日	Radiant	開発者が社内でPDFを共有したことでマルウェアが拡散され、暗号資産取引システムまで感染
トランザクション改ざん・署名誘導 ❺	2024年10月16日 14:47(UTC)	Radiant	作成された送金トランザクションは改ざんされており、HWウォレットに到達したトランザクションには、自己資金を保管する融資用プールのコントロールを委譲する関数が含まれていた
トランザクション改ざん・署名誘導 ❻	2024年10月16日 14:47(UTC)	Radiant	作成された送金トランザクションは改ざんされており、HWウォレットに到達したトランザクションには、自己資金を保管する融資用プールのコントロールを委譲する関数が含まれていた
トランザクション改ざん・署名誘導 ❼	2024年10月16日 14:47(UTC)	Radiant	PC上では正常な取引であるように表示されており、全容を確認せずにHWウォレット（Ledger）で改ざんトランザクションに署名
トランザクション改ざん・署名誘導 ❽	2024年10月16日 14:47(UTC)	Radiant	PC上では正常な取引であるように表示されており、全容を確認せずにHWウォレット（Ledger）で改ざんトランザクションに署名
トランザクション改ざん・署名誘導 ❾	2024年10月16日 14:47(UTC)	Radiant	署名が完了すると、改ざんトランザクションがブロックチェーンにブロードキャストされた
資金流出 ❿	2024年10月16日 17:09(UTC)	Radiant	改ざんトランザクションにより、融資用プールの権限を奪取され、資金が流出した

参考：「Anatomy of a $53 Million Hack: How Radiant Capital's Multisig Failed」（CoinsBench/Marcellus Nwankwo）2026年3月時点

本事案は、開発者へのソーシャルエンジニアリングと マルウェアによる攻撃を通じてトランザクションが改ざんされ、資金が窃取された事例である

主要な事実関係と考えられる脆弱性・対策（1/2）

	事実	インシデントにつながった脆弱性	実施すべきだった対策	参考：MITRE ATT&CKの攻撃技法	参考：MITRE AADAPTの攻撃技法	参考：MITRE D3FENDの防御技法
Radiant Capital	Radiant Capital社（以下、Radiant）は分散型クロスチェーンを利用した融資（DeFi）を提供					
攻撃者	以下のマルウェアを準備し、同社の元の外部委託者を偽装してTelegramで連絡をした ① PDFファイルに偽装した実行ファイルであり、開くと専門的かつ詳細なPDFファイルが表示されるが、マルウェアによりバックドアが設定される	外部連絡先確認・フィッシング対策が不十分	■ 取引先確認・別経路確認・フィッシング対策の教育・訓練	フィッシング (T1566)	アカウント取得 (ADT3001) 外部サービスの悪用 (ADT3008)	メッセージ分析 (D3-MA) ユーザー行動分析 (D3-UBA)
	② 感染したPCの通信を傍受	通信保護・端末信頼性確認が不十分	■ 専用署名端末、通信認証、証明書ピンニング	ネットワークスニッフィング (T1040) 中間者攻撃 (T1557)	アカウント取得 (ADT3001)	資格情報送信範囲制御 (D3-CTS) メッセージ認証 (D3-MAN)
	③ 感染PC上でウォレット操作が行われると、トランザクションが改ざんされ、HWウォレットに到達したトランザクションには貸出プールのコントロールを委譲する関数が含まれている	未署名Txの改ざん防止機能が不十分	■ Txハッシュ照合、署名前検証、独立端末での確認	送信データの改ざん (T1565.002)	スマートコントラクト実装の悪用 (ADT3012)	取引コンテキスト検証 (D3-TV) ファイルメタデータ整合性検証 (D3-FMCV)
	④ PC上では正常な取引であるかのように表示	UI表示への過度な信頼 ブラインド署名(*1)	■ HWウォレット表示内容確認、二経路確認	偽装 (T1036)	ブラインド署名 (ADT3012.006相当)	コンテンツ検証 (D3-CV) ドメインロジック検証 (D3-DLV)

(*1): スマートコントラクトを含む複雑なトランザクション等に対して、ユーザーが署名内容の全容を画面上で確認できずに署名すること（P65参照）

本事案は、開発者へのソーシャルエンジニアリングと マルウェアによる攻撃を通じてトランザクションが改ざんされ、資金が窃取された事例である

主要な事実関係と考えられる脆弱性・対策（2/2）

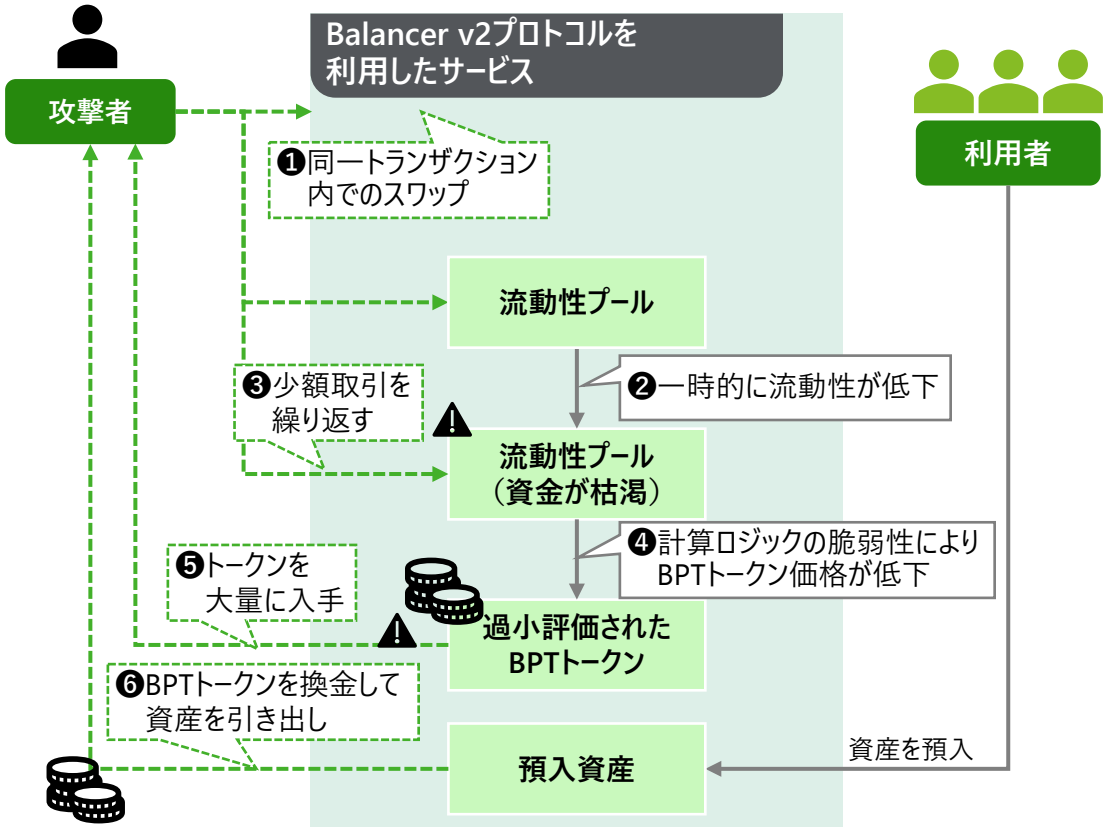
	事実	インシデントにつながった脆弱性	実施すべきだった対策	参考：MITRE ATT&CKの攻撃技法	参考：MITRE AADAPTの攻撃技法	参考：MITRE D3FENDの防御技法
Radiant Capital	① 開発者が社内でPDFを共有することでマルウェアが拡散し、送金業務に携わる担当者のPCが感染した	ファイル実行制御・検査が不十分 ユーザー実行対策・EDRが不十分 社内ファイル共有・横展開対策が不十分	■ 添付ファイル隔離、実行ファイル制限 ■ EDR、アプリケーション制御、ユーザー教育 ■ 共有ファイル検査、端末分離、送金端末の専用化	偽装 (T1036) 難読化されたファイル (T1027) ユーザーによる実行: 悪意のあるファイル (T1204.002) 内部スピアフィッシング (T1534)	アカウント取得 (ADT3001)	メッセージ分析 (D3-MA) ユーザー行動分析 (D3-UBA) ファイル分析 (D3-FA) 実行バイナリ検証 (D3-SBV)
	② 感染したPCでウォレット操作を行った。取引シミュレーション（Tenderly）も実行していた模様	マルウェア検知・端末監視が不十分	■ EDR、振る舞い検知、永続化検知、端末隔離	侵入ツールの転送 (T1105) コマンド及びスクリプト解釈 (T1059)		アプリケーションの強化 (D3-AH) ファイル完全性監視 (D3-FIM)
	③ HWウォレット（Ledger）で改ざんトランザクションに署名したが、全容を確認せずに署名した	ブラインド署名(*1) 権限変更Txの検証不足	■ HWウォレット表示内容確認、二経路確認 ■ 権限変更の高リスク判定、複数者承認、allowlist	偽装 (T1036) 送信データの改ざん (T1565.002)	ブラインド署名 (ADT3012.006相当) コントラクトの所有権変更 (ADT3012.001)	コンテンツ検証 (D3-CV) ドメインロジック検証 (D3-DLV) 構成権限制御 (D3-SCP) アクセス制御 (D3-AMED)
	④ 改ざんトランザクションにより、融資用プールの権限を奪取され、資金が流出した	同一ウォレットでの資産集中管理	■ 資産分散	送信データの改ざん (T1565.002)	資金の吸い上げ (ADT3028)	ファイルメタデータ整合性検証 (D3-FMCV)

(*1): スマートコントラクトを含む複雑なトランザクション等に対して、ユーザーが署名内容の全容を画面上で確認できずに署名すること（P65参照）

本事案は、スマートコントラクトの計算ロジックにおける丸め誤差を利用してトークン価格を操作し、売却益を得た攻撃である

Balancer v2事案 全体像およびタイムライン

- Balancer v2はDEX及びその自動マーケットメーカー（AMM）のプロトコルであり、複数のプラットフォームがプロトコルを利用していた
- プロトコルはbatchSwap機能をもち、複数の流動性プールをまたいだ連続的なスワップを一つのトランザクションで実行することができた。batchSwap機能では時点決済ルールにより、トランザクション内での一時的な借入や残高不足を許容していた
- 攻撃者は、スマートコントラクトの丸め誤差を利用してトークンの価格を意図的に下落させた上でトークンを入手、売却し利益を得た



攻撃のタイムライン

No.	発生日時	主体	説明
❶	2025年11月3日 07:46(UTC)	攻撃者	時点決済ルールを悪用し、同一トランザクション内でトークンをスワップした
❷		Balancer	特定の流動性プールの資産がほぼ空になった
❸		攻撃者	そのプールの中で少額取引を繰り返した
❹		Balancer	取引の計算では端数を切り捨てていたが、該当のプールは資産が少ない（流動性が低い）ため、プールに対して切り捨てられた端数の総額の割合が増大した。その結果、プールの資産価値を示す定数の値が低下し、BPTトークン（資産の預け入れの証明）の価格が低下した
❺		攻撃者	過小評価されたBPTトークンを入手・交換し、大量の資金を得た
❻			

脆弱性を悪用した過小な価格でのトークンの入手：❶〜❹
トークンの売却：❺❻

参考：「Understanding the Balancer v2 Exploit: Technical Analysis and Lessons for the Blockchain Industry」（OpenZeppelin）2026年3月時点

本事案は、スマートコントラクトの計算ロジックにおける丸め誤差を利用してトークン価格を操作し、売却益を得た攻撃である

主要な事実関係と考えられる脆弱性・対策

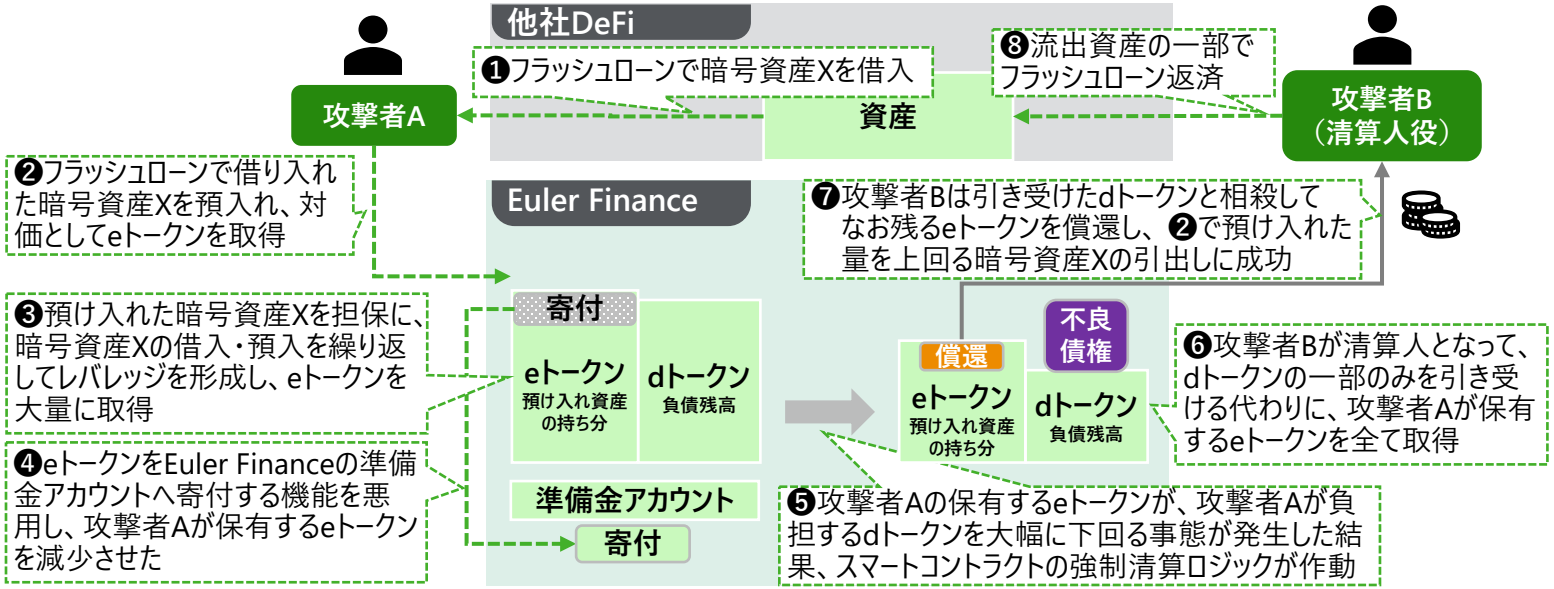
事実		インシデントにつながった脆弱性	実施すべきだった対策	参考：MITRE ATT&CKの攻撃技法	参考：MITRE AADAPTの攻撃技法	参考：MITRE D3FENDの防御技法
Balancer	■ Balancer v2はDEX及びその自動マーケットメーカー（AMM）のプロトコルである ■ batchSwap機能により、複数の流動性プールをまたいだ連続的なスワップを一つのトランザクションで実施でき、ガス代を節約できる。batchSwapでは時点決済ルールにより、トランザクション内での一時的な借入や残高不足を許容していた ■ Balancer v2のコードは複数のエンティティによるスマートコントラクト監査を受けていた (*1)					
攻撃者	① 時点決済ルールを悪用し、同一トランザクション内でトークンをスワップして、特定の流動性プールの資産をほぼ空にした ② そのプールの中で少額取引を繰り返した。取引の計算では端数を切り捨てる実装となっていた（脆弱性） ③ 該当プールは資産が少なく（流動性が低く）、②で生じた切り捨て端数の総額が、プール資産に対して相対的に無視できない水準となった ④ プールの資産価値を示す定数の値が低下し、BPTトークン（資産の預け入れの証明）の価格が低下した ⑤ 過小評価されたBPTトークンを入手・交換し、大量の資金を得た	複合機能のビジネスロジック検証不足	■ 機能組合わせを含むスマートコントラクト検証、形式検証		スマートコントラクトの実装分析(ADT3029)	ドメインロジック検証 (D3-DLV)
		異常取引・低流動性操作の防止不足	■ 流動性閾値、異常取引検知、取引上限	データ改ざん (T1565)	スマートコントラクト実装の悪用(ADT3012)	プラットフォームの監視 (D3-PM)
		丸め誤差・端数処理の検証不足	■ 端数処理レビュー、境界値テスト、経済的影響評価			
		低流動性時の安全制御不足	■ 最小流動性要件、低流動性時の制限		市場操作 (ADT3021)	
		価格算定ロジックの異常検知	■ 価格乖離監視、不変条件監視、オラクル補助検証	保存データの改ざん (T1565.001)		ファイルメタデータ整合性検証 (D3-FMCV)
		異常利益獲得時の停止機能不足	■ サーキットブレーカー、取引停止		資金の吸い上げ (ADT3028)	

(*1): 公開されているスマートコントラクト監査報告書のうち、攻撃対象となったコンポーネントComposable Stable Poolsを対象とした最新日付（2022年9月）の報告書では、端数処理を行う関数は監査の対象外となっていた

本事案は、フラッシュローンで入手した資金を用いてスマートコントラクトの脆弱性を悪用した取引を行い、資金を窃取した事例である

Euler Finance事案 全体像およびタイムライン

- Euler Finance（以下、Euler）は、ユーザーが暗号資産Xを預け入れるとその持ち分を表すeトークンを発行するDeFiプロトコルで、ユーザーがEulerから暗号資産Xを借り入れる場合には、返済義務を表すdトークンを引き受ける。
- Eulerでは、ユーザーが預け入れた暗号資産Xを担保に、暗号資産Xの借入・預入を繰り返して、レバレッジを形成できる。
- 攻撃者は、寄付後に口座の健全性確認が実行されない寄付機能コントラクトの脆弱性と、清算人が報酬を得られる仕組みを悪用し、資金を窃取した



	No.	発生日時	主体	説明
フラッシュローンによる資金調達	❶	2023年3月13日 08:50(UTC)	攻撃者A	**他社DeFiのフラッシュローンを用いて暗号資産Xを借入**
	❷		攻撃者A	借り入れた暗号資産XをEulerの攻撃者Aのアカウントへ預け、対価としてeトークンを取得
寄付機能を悪用した取引	❸		攻撃者A	預け入れた暗号資産Xを担保に、暗号資産の借入・預入を繰り返してレバレッジを形成し、eトークンを大量に取得
	❹		攻撃者A	準備金アカウントにeトークンの一部を寄付。**債務超過状態になる寄付だったがブロックされなかった**
	❺		Euler	eトークンの保有総額がdトークンの保有総額を大幅に下回る事態が発生した結果、スマートコントラクトの強制清算ロジックが作動
	❻		攻撃者B	清算人となって、dトークンの一部のみを引き受ける代わりに、攻撃者Aが保有するeトークンを全て取得
フラッシュローン返済と差額利益の窃取	❼		Euler	引き受けたdトークンと相殺してなお残るeトークンを償還し、**❷で預け入れた量を上回る暗号資産Xの引出しに成功**
	❽		攻撃者B	eトークンの償還により得た資金の一部で**フラッシュローンの借入資金を返済**

参考：「$197 Million Stolen: Euler Finance Flash Loan Attack Explained」（Chainalysis）2026年3月時点

本事案は、フラッシュローンで入手した資金を用いてスマートコントラクトの脆弱性を悪用した取引を行い、資金を窃取した事例である

主要な事実関係と考えられる脆弱性・対策

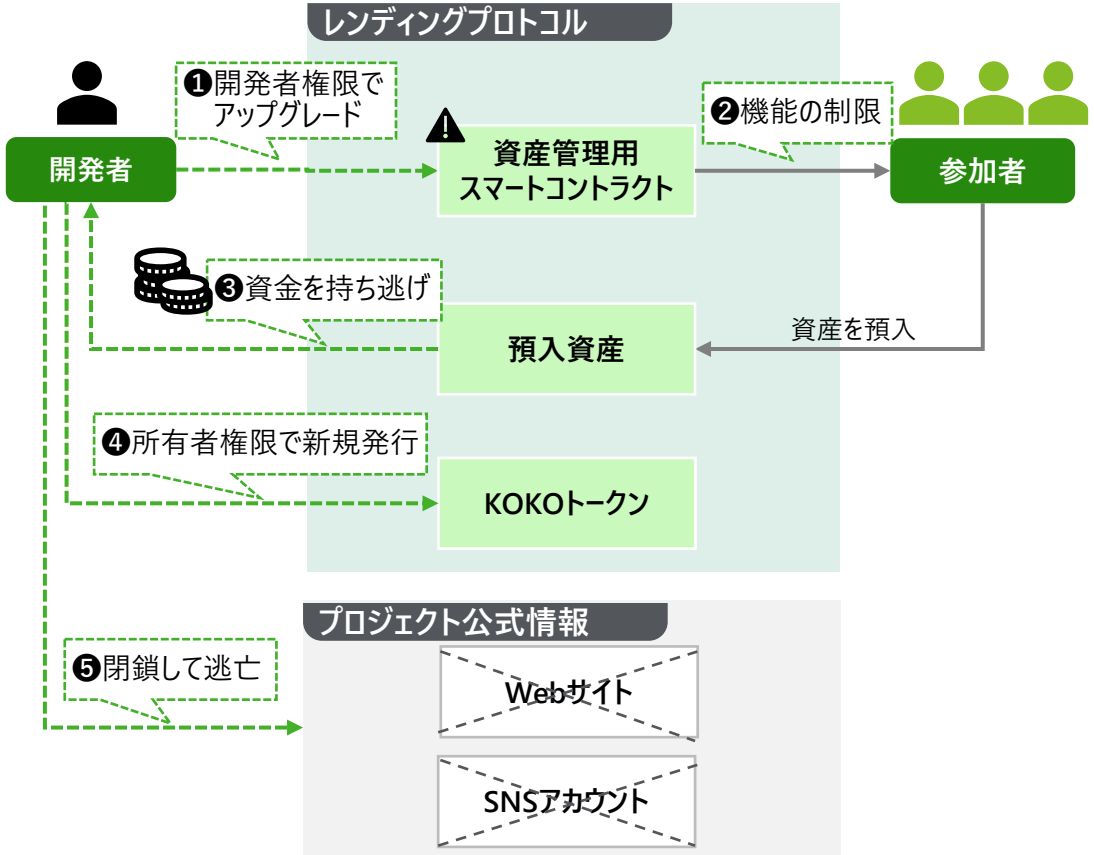
事実	インシデントにつながった脆弱性	実施すべきだった対策	参考：MITRE ATT&CKの攻撃技法	参考：MITRE AADAPTの攻撃技法	参考：MITRE D3FENDの防御技法
Euler ■ Euler Finance社（以下、Euler）は、ETHチェーン上でDeFiレンディングプロトコルを構築。利用者は暗号資産の貸付・借入を行うことができる ■ スマートコントラクトに寄付機能を追加したが、アカウントが債務超過となるような寄付をブロックするロジックが実装から漏れていた（脆弱性） ■ スマートコントラクト監査を受けていたが、寄付機能の脆弱性について指摘されなかった(*1)					
攻撃者 以下の流れで資金を窃取した。 ① 他のフラッシュローンを用いて暗号資産Xを借入 ② 借り入れた暗号資産XをEulerの攻撃者Aのアカウントへ預け、対価としてeトークンを取得 ③ 預け入れた暗号資産Xを担保に、暗号資産の借入・預入を繰り返してレバレッジを形成し、eトークンを大量に取得 ④ 準備金アカウントに債務超過状態になるeトークンの寄付を行ったが、ブロックされず、強制清算ロジックが作動 ⑤ 攻撃者は清算人としてdトークンの一部のみを引き受ける代わりに、保有していたeトークンを全て取得 ⑥ 引き受けたdトークンと相殺してなお残るeトークンを償還し、②で預け入れた量を上回る暗号資産Xの引出しに成功	大口瞬間流動性を前提としたリスク制御不足 担保トークン発行ロジックの悪用可能性 レバレッジ・負債状態の制御不足 寄付機能に債務超過防止のロジックがなかった 清算ロジックの悪用可能性検証不足 清算報酬の上限・異常検知不足 異常時の停止機能不足	■ フラッシュローン耐性検証、大口取引監視 ■ プロトコル全体の状態遷移検証 ■ ポジション上限、リスクパラメータ監視 ■ 寄付機能の安全条件検証、債務超過ロジック ■ 清算前後の不変条件検証、異常清算検知 ■ 清算報酬上限、異常報酬検知 ■ 取引時不変条件監視、緊急停止	データ改ざん (T1565)	フラッシュローン (ADT3015) スマートコントラクトの実装分析(ADT3019) スマートコントラクト実装の悪用(ADT3012) 市場操作 (ADT3021) 資金の吸い上げ (ADT3028)	プラットフォームの監視 (D3-PM) ドメインロジック検証 (D3-DLV) 取引コンテキスト検証 (D3-TV)

(*1): その後、寄付機能の脆弱性を看過した監査機関はスマートコントラクト監査の不備を認め、Euler Financeに対して賠償金を支払っている

本事案は、スマートコントラクトの開発者権限を悪用した、DeFiプロトコル開発者によるラグプル （資金持ち逃げ）の事例である

Kokomo Finance事案 全体像およびタイムライン

- Kokomo Financeプロジェクト（以下、Kokomo）は、Optimism（Ethereumのレイヤー2ネットワーク）上で、オープンソースのレンディング・プロトコルとして稼働を開始し、あわせてKOKOトークンを発行した。プロジェクトは稼働直後から大手ブロックチェーンデータプラットフォームに掲載され、多くのユーザーが資金を預け入れていた
- 突如、運営体はユーザの預託資産の転送や大量のミントにより資金を得て、姿を消した



攻撃のタイムライン

No.	発生日時	主体	説明
コントラクト改ざん ❶	2023年3月26日 09:00(UTC)	Kokomo	十分な資金が集まった段階で、KOKOトークンの開発者権限を利用し、ユーザーの預託資産を管理するスマートコントラクトを改ざん（アップグレード）
コントラクト改ざん ❷		参加者	改ざんされたスマートコントラクトによって、ユーザーは報酬の受け取りや借り入れが制限
資金流出 ❸	2023年3月26日 14:02(UTC)	Kokomo	ユーザーの預託資産を消費するように操作し、外部のアドレスへユーザーの預託資産を転送
資金流出 ❹		Kokomo	KOKOトークン所有者が、任意のアドレスに大量発行（ミント）できる機能を悪用し、新規発行により利益を得た
資金流出 ❺	2023年3月26日	Kokomo	プロジェクトに関する公式サイトやSNSアカウントを閉鎖して逃亡

参考：「Optimism DeFi Protocol Kokomo Finance Rug Pulls Users for $4 Million」（Binance News）2026年3月時点

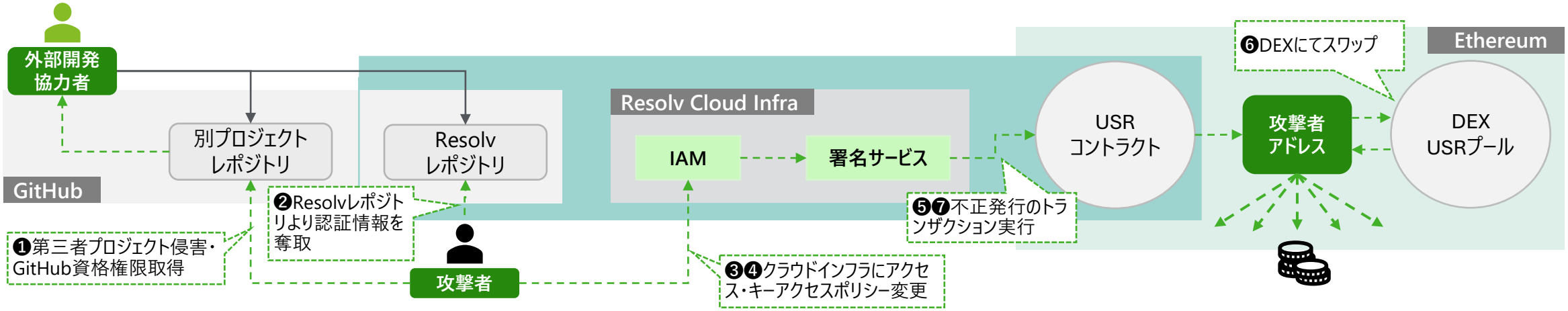
本事案は、スマートコントラクトの開発者権限を悪用した、DeFiプロトコル開発者によるラグプル （資金持ち逃げ）の事例である

主要な事実関係と考えられる脆弱性・対策

事実		インシデントにつながった脆弱性	実施すべきだった対策	参考：MITRE ATT&CKの攻撃技法	参考：MITRE AADAPTの攻撃技法	参考：MITRE D3FENDの防御技法
Kokomo Finance	■ Kokomo Financeプロジェクト（以下、Kokomo）は、Optimism（Ethereumのレイヤー2ネットワーク）上で、オープンソースのレンディング・プロトコルとして稼働を開始。あわせてKOKOトークンを発行。利用しているスマートコントラクトは監査を受けていた ■ 稼働直後から大手ブロックチェーンデータプラットフォームに掲載され、多くのユーザーが資金を預け入れる ■ 十分な資金が集まった段階で、以下のラグプルが実行された ① KOKOトークンの開発者権限を利用し、ユーザーの預託資産を管理するスマートコントラクト（後からアップグレード可能な設計であり、開発者権限があればコントラクトの更新が可能な状態であった）を改ざん ② 改ざんされたスマートコントラクトによって、ユーザーは報酬の受け取りや借り入れが制限された また、ユーザーの預託資産を消費するように操作し、Kokomoは外部のアドレスへユーザーの預託資産を転送した（持ち逃げ） ③ さらにKOKOトークン所有者が任意のアドレスに大量に新規発行（ミント）できる機能を利用して、トークンを新規発行して利益を得る ④ プロジェクトに関する公式サイトやSNSアカウントを閉鎖して逃亡した	本事案は当初から集めた資金を詐取することが目的である可能性が高く、出資者が主体的に実施するIT統制やセキュリティ対策で資金流出を防止することが困難であったと考えられるため、セキュリティ対策の考察は省略する。		データ改ざん（T1565）	市場操作(ADT3021) コントラクトの所有権変更(ADT3012.001) 偽トークン生成(ADT3016) 資金の吸い上げ(ADT3028)	構成権限制御（D3-SCP） アクセス制御（D3-AMED） ドメインロジック検証（D3-DLV）

本事案は、DeFiもコントラクト監査のみでは不十分で、GitHub、CI/CD、クラウドIAM/KMS、署名サービス等を一体で評価する必要性を示した事例である

Resolv事案 全体像およびタイムライン



		発生日時	主体	攻撃のタイムラインの説明
攻撃準備	❶	–	攻撃者	Resolvの外部開発協力者が過去に関与していた第三者プロジェクトを侵害し、当該協力者のGitHub資格権限を取得
GitHub／CI・CD侵害	❷	–	攻撃者	取得したGitHub資格情報を使い、一部レポジトリへアクセス。悪意あるworkflowを配置し、機微な認証情報を窃取
	❸	–		窃取した認証情報を用いてクラウドインフラにアクセス。サービスの列挙、APIキーの探索、権限範囲の確認等の偵察を実施
	❹	–		インフラ権限のポリシー管理機能を使い、キーアクセスポリシーを変更してミント完了処理に使われる署名権限を取得
署名権限奪取／不正ミント	❺	2026年3月22日 02:21(UTC)		Resolvのコントラクトに対して１回目の不正トランザクションを実行。10万USDCを預入れ、5,000万USRを不正ミント
	❻	2026年3月22日 02:21～03:41 (UTC)		不正ミントしたUSRを複数ウォレットと多数のDEXスワップを使ってETH等へ変換
	❼	2026年3月22日 03:41 (UTC)		Resolvのコントラクトに対して２回目の不正トランザクションを実行。10万USDCを預入れ、3,000万USRを不正ミント
インシデント対応		2026年3月22日 05:16/05:30 (UTC)	Resolv	リアルタイム監視により異常トランザクションを検知した上で、関連コントラクトを全て停止・侵害された認証情報を無効化
		–		CI/CD・クラウドAPIキー・認証サービス・VPN等の認証情報をローテーション。約4,600万USRを凍結

※各事例に関して公表されている資料及び本報告書の執筆時点で入手可能な情報に基づき調査研究の目的から整理したもので、個別事案に関する責任の所在又は法的評価を示すものではありません

【参考】Resolv Postmortem: March 22, 2026 Incident

本事案は、DeFiもコントラクト監査のみでは不十分で、GitHub、CI/CD、クラウドIAM/KMS、署名サービス等を一体で評価する必要性を示した事例である

主要な事実関係と考えられる脆弱性・対策（1/2）

事実	インシデントにつながった脆弱性	実施すべきだった対策	参考：MITRE ATT&CKの攻撃技法	参考：MITRE AADAPTの攻撃技法	参考：MITRE D3FENDの防御技法
外部協力者 ■ 外部開発協力者が関与する別のプロジェクトへの侵害により、当該協力者のGitHub資格情報が奪取された ■ GitHub資格情報を足場として、ResolvのGitHubリポジトリへの初期アクセスが行われた	外部協力者権限が過大 資格情報の失効・棚卸し不足	■ 外部協力者アクセスをJIT化・最小権限化 ■ fine-grained token /MFA/PAT禁止 ■ プロジェクト終了時の即時失効、外部協力者権限期限管理	有効なアカウント (T1078)	アカウント取得 (ADT3001) 外部サービスの悪用 (ADT3008) 資金の吸い上げ (ADT3028)	アクセス制御 (D3-AMED) クレデンシャルの強化 (D3-CH) 資格情報ローテーション (D3-CRO) 多要素認証 (D3-MFA) ユーザー権限管理 (D3-UAP)
■ GitHub workflowを悪用して機微な認証情報を窃取した上で、窃取した認証情報でクラウド環境に入り、APIキーやサービス構成を偵察	CI/CD credential保護不足 GitHub workflow変更監視不足	■ OIDC等の短命認証へ移行、CI/CD認証チェーンから署名操作を遮断、workflow変更へのレビュー必須化	アプリケーションアクセストークンの窃取(T1528) サプライチェーン侵害 (T1195)	サプライチェーン侵害 (ADT1195)	構成権限制御 (D3-SCP) 資格情報ローテーション (D3-CRO)
	クラウド認証情報の横展開可能性 クラウドAPI利用・権限行使の異常検知不足	■ クラウド権限分離、条件付きアクセス、JIT ■ API利用監視、権限行使アラート、構成変更監視	有効なアカウント: クラウドアカウント (T1078) クラウドサービスダッシュボードの利用 (T1538) アカウント探索 (T1087)	外部サービスの悪用 (ADT3008)	アクセス仲介 (D3-AMED) リソースアクセスパターン分析 (D3-RAPA) プラットフォームの監視 (D3-PM)

本事案は、DeFiもコントラクト監査のみでは不十分で、GitHub、CI/CD、クラウドIAM/KMS、署名サービス等を一体で評価する必要性を示した事例である

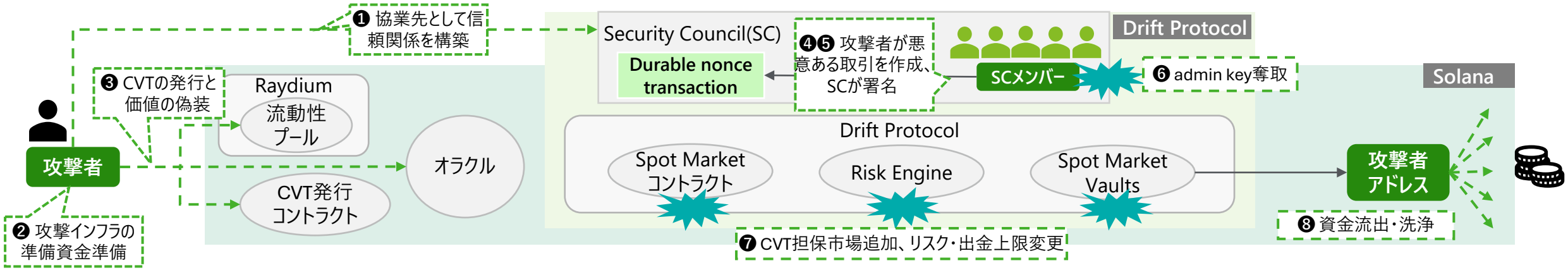
主要な事実関係と考えられる脆弱性・対策（2/2）

事実		インシデントにつながった脆弱性	実施すべきだった対策	参考：MITRE ATT&CKの攻撃技法	参考：MITRE AADAPTの攻撃技法	参考：MITRE D3FENDの防御技法
攻撃者	■ KMS key policy変更により署名権限を取得	KMS権限分離が不十分	■ KMS policy変更の二者承認・職務分掌 ■ KMS key policy変更イベント即時検知	追加クラウドロール付与 (T1098.003) 有効なアカウント (T1078)	アカウント取得 (ADT3001) 内部者利用 (ADT3017)	構成権限制御 (D3-SCP) アクセス制御 (D3-AMED)
	■ completeSwapでUSRを不正ミント	オフチェーン署名権限への依存	■ 署名鍵の閾値化・複数者承認 ■ 署名対象の取引コンテキスト検証 ■ 高リスク操作時の自動権限失効	データ改ざん (T1565)		ドメインロジック検証 (D3-DLV) アクセス制御 (D3-AMED) 取引コンテキスト検証 (D3-TV)
		ミント上限・価格検証が不十分	■ ミント上限設定／オラクル価格検証 ■ 異常ミント検知と自動停止 ■ 発行量・担保価値の不変条件監視		偽トークン生成 (ADT3016) 資金の吸い上げ (ADT3028)	

本事案は、長期のソーシャルエンジニアリングと事前署名により、プロトコル管理権限が奪われ、偽担保による借入が可能となり、資産が流出した事例である

Drift事案 全体像およびタイムライン

- 攻撃者は、Drift Protocol関係者への長期的な信頼形成を通じて、Solanaのdurable nonceを用いた事前署名を取得
- Drift Protocolのadmin権限を奪取した上で、攻撃者が発行する無価値のトークンを担保とすることを有効化し、USDC・SOL等のトークンを引き出した



	No.	発生日時	主体	攻撃のタイムラインの説明
攻撃準備	❶	2025年秋頃～2026年春	攻撃者	Drift関係者と国際会議やTelegram等で接触。Vaultのオンボードや$1M超の預入等で協業先として信頼を形成
	❷	2026年3月11日	攻撃者	Tornado Cash由来の10 ETHを引き出し、攻撃インフラ・偽担保作成の準備資金として利用
	❸	2026年3月12日頃	攻撃者	CarbonVote Token（CVT）を作成し約7.5億枚をミント。DEXのRaydium上で少額流動性を置き、自己取引により$1近辺の価格を偽装。攻撃者管理のオラクルでDrift側に価格情報を供給
管理権限奪取	❹	2026年3月23日～30日	攻撃者 / Drift	durable nonce accountを作成し、Security Council署名者からadmin移転等を含む事前署名を取得
	❺	2026年3月26日～27日頃	Drift	Security Council が2-of-5マルチシグ・ゼロタイムロック構成へ移行。攻撃者は新構成でも必要署名を確保
	❻	2026年4月1日16:05（UTC）	攻撃者	事前署名済みtransactionを実行し、admin keyを攻撃者管理アドレスへ移転
資産流出	❼	直後	攻撃者	CVTを担保市場に追加し、リスク・出金上限を変更。5億CVTを預け入れ
	❽	～18:31頃（UTC）	攻撃者	31本の出金で実資産を流出、出金した資金をSolana上で交換、Ethereum等へブリッジ後、ETH化・分散

【参考】Incident Recovery Update – April 16, 2026

本事案は、長期のソーシャルエンジニアリングと事前署名により、プロトコル管理権限が奪われ、偽担保による借入が可能となり、資産が流出した事例である

主要な事実関係と考えられる脆弱性・対策（1/2）

	事実	インシデントにつながった脆弱性	実施すべきだった対策	参考：MITRE ATT&CKの攻撃技法	参考：MITRE AADAPTの攻撃技法	参考：MITRE D3FENDの防御技法
Drift	■ durable nonce accountを作成 ■ routineに見えるTxに事前署名 ■ 実際にはadmin移転等を含むblind signing	ブラインド署名(*1) durable nonceの制御が不十分	■ 専用署名端末、取引データデコード ■ 重要アクションでdurable nonceを禁止		署名再利用・遅延実行 (ADT3012.006類似) 所有権変更 (ADT3012.001)	取引コンテキスト検証 (D3-TV) 資格情報送信範囲制御(D3-CTS)
	■ 2-of-5・ゼロタイムロックへ移行 ■ 事前署名済みTxでadmin keyを移転	閾値・タイムロックが不十分 admin移転先の制御が不十分	■ 3-of-5/4-of-7等への閾値強化 ■ 重要操作への24～72時間timelock ■ admin移転先allowlist・リアルタイム警告		所有権変更 (ADT3012.001)	構成権限制御 (D3-SCP) アクセス制御 (D3-AMED) 認可イベント閾値監視 (D3-AZET)
	■ CVTを担保市場に追加 ■ borrow limitやrisk parameterを緩和 ■ 5億CVTを約$500M相当担保として認識	リスクパラメータ変更制限が不十分 新規担保の初期上限が不十分	■ 担保factor/借入capの段階的引上げ ■ 新規市場追加・オラクル指定・リスク変更に関する権限分離		スマートコントラクト実装悪用(ADT3012) オラクル操作 (ADT3012.004)	コンテンツ検証 (D3-CV) ファイルメタデータ整合性検証 (D3-FMCV)
	■ 出金上限・サーキットブレーカーを緩和 ■ 31本の出金でJLP・USDC・SOL等が流出 ■ 約2.5時間、資産移動が継続	出金上限変更の制限が不十分 異常時の自動停止が不十分	■ パラメータ変更倍率制限 ■ 複数市場同時変更の禁止 ■ 異常大口出金検知時の自動停止		出金制限回避 (ADT3004.002)	インバウンドセッション量分析 (D3-ISVA) 資源アクセスパターン分析(D3-RAPA)

(*1): スマートコントラクトを含む複雑なトランザクション等に対して、ユーザーが署名内容の全容を画面上で確認できずに署名すること（P65参照）

本事案は、長期のソーシャルエンジニアリングと事前署名により、プロトコル管理権限が奪われ、偽担保による借入が可能となり、資産が流出した事例である

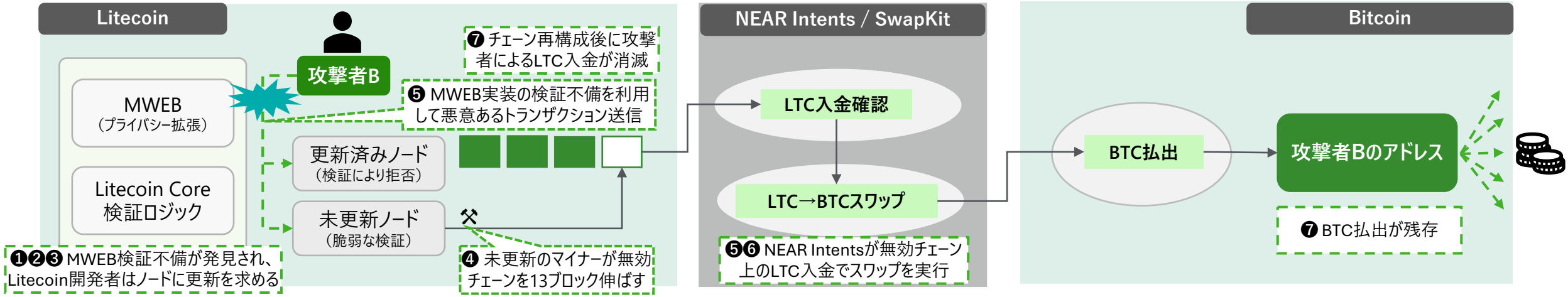
主要な事実関係と考えられる脆弱性・対策（2/2）

	事実	インシデントにつながった脆弱性	実施すべきだった対策	参考：MITRE ATT&CKの攻撃技法	参考：MITRE AADAPTの攻撃技法	参考：MITRE D3FENDの防御技法
攻撃者	■ 量的取引会社を装い、Drift関係者と長期接触 ■ Vaultオンボードや$1M超の預入等で信頼を形成	人間系・取引先確認が不十分	■ 署名者向けソーシャルエンジニアリング訓練 ■ 署名依頼の業務フロー分離・二経路確認		ソーシャルエンジニアリング権限奪取の準備段階	メッセージ分析 (D3-MA) 利用者行動分析 (D3-UBA) ネットワークトラフィック分析 (D3-NTA)
	■ CVTを作成し約7.5億枚をミント ■ 少額流動性・自己取引で$1近辺の価格を偽装 ■ 攻撃者管理オラクルが当該価格を参照	新規担保審査が不十分 オラクル・流動性検証が不十分	■ 最低流動性・保有分散・取引期間要件 ■ 複数オラクル、異常価格の自動拒否等		偽トークン生成 (ADT3016) オラクル操作 (ADT3012.004)	ネットワークトラフィック分析 (D3-NTA) ドメインロジック検証 (D3-DLV) ファイルメタデータ整合性検証 (D3-FMCV)

本事案は、チェーンのreorgリスクを前提とした設計なしでは、無効チェーン上の入金が第三者スワップを通じて実損に転化することを示した事例である

Litecoin/Near intents事案 全体像およびタイムライン

- 攻撃者は、Litecoinチェーンで発生するブロックチェーンの分岐を悪用し、将来無効となる分岐チェーン上でNear IntentsへLTC（暗号資産）の入金を行った。
- Near IntentsはLTCの入金を確認済みと判断し、Bitcoin側で攻撃者にBTCを引き渡した。
- しかしその後、Litecoinチェーンの分岐が修正され、当初のLTCの入金は無効化された結果、攻撃者はLTCを支払わずにBTCだけを取得した。



	No.	発生日時	主体	攻撃のタイムラインの説明
	❶	2026年3月19日	LTC開発者/マイナー	内部レビューでMWEB検証不備を把握。チェーンスキャンによって、あるブロックで約85,000LTCの不正peg-out発生を確認
	❷	2026年3月19日～24日		Litecoin Foundationは、マイナー限定の緊急リリースを展開し、攻撃者Aのoutpointを一時凍結
	❸			攻撃者Aが資金返還に協力。返還額をMWEBへpeg-inし、rebalancing outputを凍結して会計上の不均衡を解消
	❹	～2026年4月25日		更新済みマイナーが正常採掘を継続しにくい間、MWEB修正を適用していないマイナーが無効チェーンを13ブロック分延伸
無効チェーン上でスワップ	❺	2026年4月25日 8:40:16（UTC）	攻撃者B	無効チェーン上のLTC入金を用いてNEAR Intents/SwapKitでLTC→BTCのスワップを作成・処理し、BTC払出しまで完了
	❻	2026年4月25日 8:51:13（UTC）	攻撃者B	追加のLTC→ETHのスワップを試行。ただし、当該スワップは失敗（failed）となり、追加被害は防止された可能性
Reorg	❼	2026年4月25日	LTCマイナー	正規チェーンが無効チェーンを上回り、13の不正ブロックをreorgで無効化

【参考】Litecoin MWEB Security Incident Postmortem

本事案は、チェーンのreorgリスクを前提とした設計なしでは、無効チェーン上の入金が第三者スワップを通じて実損に転化することを示した事例である

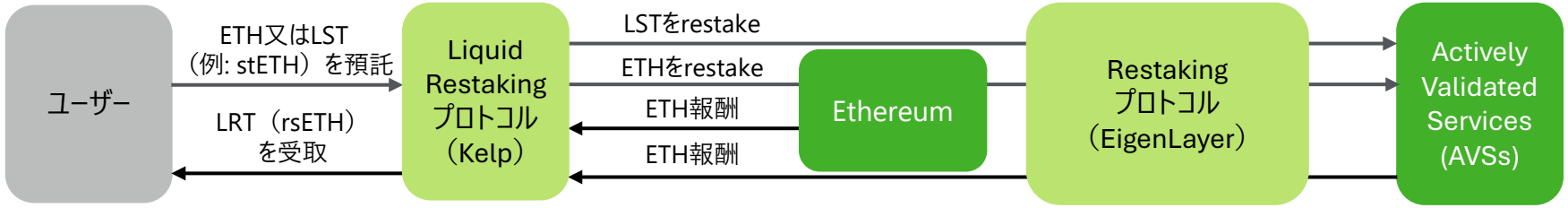
主要な事実関係と考えられる脆弱性・対策

	事実	インシデントにつながった脆弱性	実施すべきだった対策	参考：MITRE ATT&CKの攻撃技法	参考：MITRE AADAPTの攻撃技法	参考：MITRE D3FENDの防御技法
Litecoin	■ MWEB inputが参照するUTXOメタデータを偽装し、検証ロジックに対して少額inputが大きなoutput相当を裏付ける価値を持つように見せることが可能だった ■ 更新済みノードは不正ブロックを拒否するも、MWEBブロックデータを保持する挙動により、後続の正当なブロック処理のマイニングRPCが阻害された	メタデータ検証漏れ パッチ充てのラグ マイナー間の緊急調整への依存	■ 公開パッチのみならず、マイナー／ノードの実効アップグレード率を監視	データ改ざん (T1565) エンドポイントサービス妨害 (T1499)	チェーン固有仕様の悪用（ADT3013）	ドメインロジック検証 (D3-DLV) 運用ロジック検証 (D3-OLV) ソースコードの堅牢化 (D3-SCH) ネットワーク分離 (D3-NI)
	■ 正規チェーンが無効チェーンを上回った後、13の無効なブロックがreorgされ、Litecoin側の入金は消滅した	Reorg/Fork耐性・Finality評価が不十分	■ 不正チェーン／フォーク監視 ■ マイナーへの緊急連絡経路の確保 ■ 正規チェーンへの再収束の手順準備 ■ reorg耐性を踏まえ確認数を固定値ではなくリスクに連動化 ■ PoW Finalityに応じた確認数引上げ ■ スワップ上限・遅延決済			取引コンテキスト検証 (D3-TV) ファイルメタデータ整合性検証 (D3-FMCV) ネットワークトラフィック分析 (D3-NTA)
Near Intents/攻撃者	■ NEAR Intents/SwapKitは、無効チェーン上のLTC入金を確認し、スワップとBTC払出を完了した ■ 攻撃者は、13の無効なブロックがreorgで排除される前に、無効チェーン上のLTCをクロスチェーンスワップの入金として利用した	無効ブロックの入金確認を信頼 上限・一時停止条件が不十分		資金の吸い上げ (ADT3028) クロスチェーンスワップ (ADT3005)		アクセス制御 (D3-AMED) インバウンドセッション量分析 (D3-ISVA) 運用ロジック検証 (D3-OLV) ネットワーク分離 (D3-NI) 取引コンテキスト検証 (D3-TV)

本事案は、クロスチェーン検証の脆弱性を突かれ、正当な発行条件を満たさないLRTのrsETHが不正発行され、DeFi市場にリスクが波及した事例である

Kelpの仕組み

■ KelpはEthereum上でLiquid Restakingプロトコルを提供。ユーザーは、同プロトコルにETHやLSTを預託し、見返りにrsETH（※LRT）を受取。rsETHは、ユーザーがKelpに預託したETHやLSTが生み出すStaking及びRestaking報酬に対する経済的持分を表し、ユーザーはこれを通じて報酬を享受。ユーザーは、Kelpに預託したETHやLSTが生み出すStaking・Restaking報酬を狙いながら、rsETHを他のDeFi市場にて担保・流動性供給・運用に回すことが可能。



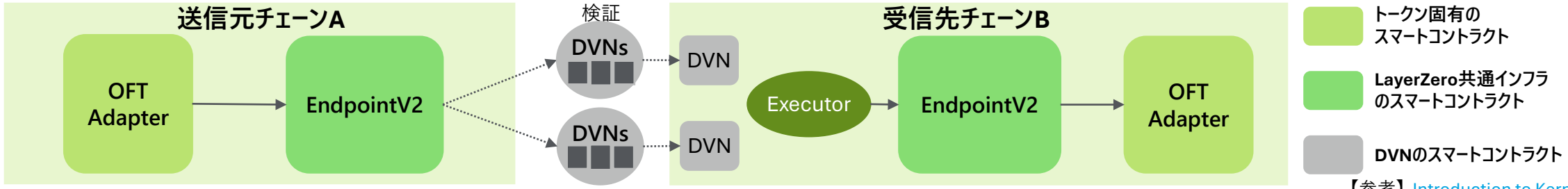
注：Liquid Staking: ETHをEthereumへのStakingのために預けつつ、その見返りとしてLSTを受け取る仕組み
： Restaking: Ethereumで既にStakeされているETHを、追加のスラッシング条件を課し、別の分散型サービス（AVS）に再ステーキングさせる仕組み
： Liquid Restaking: ETH／LSTをAVSへのRestakingのために預けつつ、その見返りとしてLRTを発行する仕組み
： Actively Validated Service（AVS）：Ethereumが持つ多数のバリデーターに依存して自らのサービスを安全に運営しようとする分散型サービス

LayerZero Omnichain Fungible Token（OFT）の仕組み

■ LayerZero（クロスチェーン技術開発・提供者）のOFTは、１つのトークンを複数チェーンに跨って動かし、全体のトークン供給量を維持するための標準
■ 同標準下において、通常の場合、LayerZeroを用いたクロスチェーンでのトークン移転は以下のとおりに動作する

① チェーンAのOFT Adapter（スマートコントラクト）がトークンをburn／lock、呼び出されたEndpointV2 （スマートコントラクト）がメッセージパケットを作成
② Decentralized Verifier Network（DVN）にて、チェーンBに転送するメッセージを検証
③ 指定されたDVN全てがチェーンB上のDVNコントラクトへ検証結果を提出後、その検証結果を用いてチェーンB上のExecutorがEndpointV2 （スマートコントラクト）を呼出
④ EndpointV2 （スマートコントラクト）が関数を呼出し、OFT Adapter （スマートコントラクト）にてトークンがmint／unlockされる

注：DVNとは、異なるブロックチェーン間で送受信されるメッセージの真正性と完全性を検証する独立した仕組みで、複数ノードにより構成される。DVNの構成については、トークン発行体側でセキュリティ要件を自由に設定可能

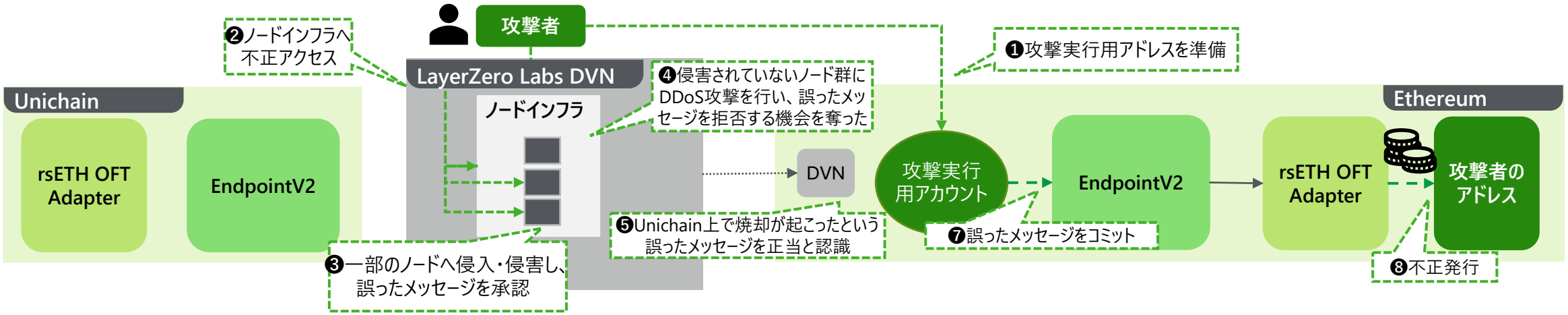


【参考】Introduction to KernelDAO
LayerZero V2 OFT Quickstart

本事案は、クロスチェーン検証の脆弱性を突かれ、正当な発行条件を満たさないLRTのrsETHが不正発行され、DeFi市場にリスクが波及した事例である

Kelp/LayerZero事案 全体像およびタイムライン

■ 攻撃者は、Unichain上でrsETHが焼却されたように見せかける偽情報を作成して、Ethereumへその情報を伝達する役割を担うノードを誤認させた。
その結果、実際にはUnichain上での正当な焼却処理が無いにも関わらず、Ethereum上で攻撃者のアドレスへ不正にrsETHが発行された。



	No.	発生日時	主体	攻撃のタイムラインの説明
攻撃準備	❶	2026年4月18日 8:39:59（UTC）	攻撃者	攻撃実行用アカウントにTornado Cash由来の資金入金が行われる
不正アクセスとDDoS攻撃	❷	～ 17:20:00	攻撃者	LayerZero Labs DVNが参照するノードインフラ構成情報にアクセス
	❸			一部のノードへ侵入・侵害し、誤ったメッセージを承認
不正メッセージを用いた関数呼出	❹	17:20:00 ～	攻撃者	未侵害の正常RPCノード群に対してDDoS攻撃を実施。DVNのRPCアクセスがタイムアウトしてフェイルオーバーが発生 DVNは侵害済みRPCノードへの問い合わせに依存する状態に遷移
	❺	17:33:35	LayerZero /Kelp	DVNの侵害済みRPCは、実際には未発生のクロスチェーン取引が存在したかのようなメッセージを返却 LayerZero Labs DVNは正規でないメッセージを正当と認識
	❻	17:35:11	攻撃者	Ethereum上で攻撃実行用アカウントを用いてDVN検証済みの状態をEndpointV2にコミット
不正流出	❼	17:35:35	攻撃者	rsETH OFT Adapterに対して正規ではない発行指示が到達し、裏付資産のない約116,500rsETHが不正に発行される

【参考】KelpDAO Incident Statement _2026年4月現在

本事案は、クロスチェーン検証の脆弱性を突かれ、正当な発行条件を満たさないLRTのrsETHが不正発行され、DeFi市場にリスクが波及した事例である

主要な事実関係と考えられる脆弱性・対策 （1/2）

	事実	インシデントにつながった脆弱性	実施すべきだった対策	参考：MITRE ATT&CKの攻撃技法	参考：MITRE AADAPTの攻撃技法	参考：MITRE D3FENDの防御技法
LayerZero Labs	■ OApp/OFT開発者（トークン発行体など）がDVN設定をカスタマイズすることを可能としており、単一DVN設定（1-of-1 DVN）にのみ依存する設定を認めていた	DVN設定の制限が不十分	■ マルチDVN化やRPC経路の明示を推奨ではなく必須に		チェーン固有仕様の悪用 (ADT3013)	ネットワーク分離 (D3-NI)
	■ LayerZero Labs DVNが依拠するRPC経路が汚染されたが、監視系には別の正常データを返していたため、異常を検知しきれなかった	監視系の独立性・多重検証不足	■ ノードバイナリ改変の監視 ■ 複数ソース検証 ■ 内部脅威・横断観測対策 ■ 追加的整合性検証		外部サービスの悪用 (ADT3008)	ファイルメタデータ整合性検証 (D3-FMCV) ネットワークトラフィック分析 (D3-NTA) トラフィック分析 (D3-RTA)
	■ 汚染されたRPCがDVNへ不正データを返した	DVN検証結果への過度な依存 完全性担保不足	■ 複数RPC検証 ■ メッセージ認証、改ざん耐性	データ改ざん (T1565) 中間者攻撃 (T1557)	チェーン固有仕様の悪用 (ADT3013)	メッセージ耐改ざん (D3-MH) メッセージ認証 (D3-MAN)
Kelp DAO	■ LayerZero Labs DVNに依存した設定を選択した	単一DVN構成への依存 DVN設定公開が不十分	■ マルチDVN化 ■ 明示的にRPC経路をConfig化			

DeFiにおけるサプライチェーン依存のリスクの存在と委託先管理の必要性が明らかとなった事案と言える。

有識者

本事案は、クロスチェーン検証の脆弱性を突かれ、正当な発行条件を満たさないLRTのrsETHが不正発行され、DeFi市場にリスクが波及した事例である

主要な事実関係と考えられる脆弱性・対策 （2/2）

	事実	インシデントにつながった脆弱性	実施すべきだった対策	参考：MITRE ATT&CKの攻撃技法	参考：MITRE AADAPTの攻撃技法	参考：MITRE D3FENDの防御技法
攻撃者	■ LayerZero Labs DVNが参照するRPCインフラ構成情報へアクセスした	RPC構成情報が推測可能	■ RPC構成情報の秘匿化、アクセス制御、構成公開範囲制限	クラウドサービスダッシュボード (T1538) 有効なアカウント (T1078)	外部サービスの悪用 (ADT3008)	構成権限制御 (D3-SCP) クレデンシャルの強化 (D3-CH)
	■ 外部RPCノード群を攻撃対象として選択し、独立した別クラスタ上で稼働していた 2 つのRPCノードに侵入した上で、0p-gethバイナリを差替えた	外部RPC依存のリスク評価不足 RPCノードの侵入対策不足 実行バイナリ完全性検証不足	■ RPC経路の明示管理、外部依存先リスク評価 ■ ノード強化、アクセス制限、侵入検知 ■ 実行バイナリの完全性検証改ざん検知	公開アプリケーションの悪用 (T1190) システムイメージの改変 (T1601) ソフトウェアバイナリの侵害 (T1554)	外部サービスの悪用 (ADT3008) サプライチェーンの侵害 (ADT1195)	リソースアクセスパターン分析 (D3-RAPA) アクセス制御 (D3-AMED) 実行バイナリ検証 (D3-SBV) ファイル完全性監視 (D3-FIM)
	■ 正常RPCノード群に対してDDoS攻撃を行った	可用性防御が不十分	■ DDoS攻撃検知ロジック冗長RPC	ネットワークサービス妨害 (T1498)	外部サービスの悪用 (ADT3008)	インバウンドトラフィックフィルタリング (D3-ITF) インバウンドセッション量分析 (D3-ISVA)
	■ DVN検証済みの状態をEndpointV2にコミット	追加的整合性検証不足	■ 事象の追加的な整合性検証 ■ 侵害RPCへの自動収束防止 ■ 時間的遅延の許容	データ改ざん (T1565)	チェーン固有仕様の悪用 (ADT3013)	ドメインロジック監視 (D3-DLV) ネットワークトラフィック分析 (D3-NTA)
	■ rsETH OFT Adapterで不正にトークン発行	発行制限・管理設計が不十分	■ トークン発行に対するレート制限や上限管理等の設計実装		偽トークン生成 (ADT3016) 資金の吸い上げ (ADT3028)	インバウンドセッション量分析 (D3-ISVA)

本事案は、クロスチェーン検証の脆弱性を突かれ、正当な発行条件を満たさないLRTのrsETHが不正発行され、DeFi市場にリスクが波及した事例である

Kelp/LayerZero事案後の主要DeFiプロトコルへの影響と対応

- 不正発行されたrsETHが担保に差し出されたAaveでは、rsETH/wrsETH市場の凍結、WETH・主要SC市場の利用率急上昇、引出不能、借入金利上昇、不良債権懸念が発生
- LayerZero LabsのRPC環境等への信頼が揺らぎ、rsETHに直接的なエクスポージャーを持っていないDeFiプロトコルがブリッジの一時停止や使用するブリッジの変更を決定
- DeFi Unitedの枠組みにより、補填資金確保、攻撃者ポジションの清算、rsETH回復計画が段階的に進められた

プロトコル	影響	対応
Kelp LayerZero	■ rsETHを担保等に使用していたレンディング・利回り市場へ信用リスクが波及した結果、rsETHのETH等価性が大きく崩れ（事案発生から約1週間で１rsETH＝約0.8795ETH）、資産価値-18.5%減	■ 緊急マルチシグによりブリッジ機能を全て凍結（Kelp） ■ 追加約200M規模の流出を阻止したことも含め、事案の発生を同日に公表（Kelp） ■ 侵害されたRPC系統との切り離しと侵害環境の再構築、1-of-1 DVN構成の禁止方針変更（LayerZero） ■ 2026年5月25日、約20,373rsETHをOFT Adapterへ補充し、回復計画を完了（Kelp）
Aave	■ 攻撃者が、不正発行の116,500rsETHのうち、Aaveに89,567rsETHを担保として、82,650WETHと821wstETHを借入れ。その結果、WETH市場及び主要SC市場で利用率が100%近くに達し、引出不能・流動性逼迫が発生 ■ rsETHの価格下落で清算人が受け取る担保価値が不確実となった結果、清算遅延が発生し、不良債権懸念が拡大（不良債権は初期推計では$123.7M～$230.1M、後続報道では約$190M規模として整理される例もある） ■ WETHの流動性枯渇により、他の安全資産を引き出すユーザー行動が誘発された結果、USDCの流動性も枯渇し、わずか24時間でUSDCの供給と借入がそれぞれ約$60M減少。TVL（預入資産価値）は48時間で$8.5B減少 ■ Aaveへの信用不安により、AAVE価格は数日で20%超下落 ※ Aaveでは、基本的には、Health Factor（=担保価値×清算閾値÷借入額）が１未満となると清算対象となる。第三者の清算人が借手の負債を肩代わり返済し、その見返りに担保＋清算ボーナスを受け取る。	■ Aaveは、ステーブルコインを含む他の流動性プールへの波及を防ぐため、WETHプールを凍結 ■ Circleの個人が、新しい貸出を呼び込み出金待ちを解消するため、金利を上げるガバナンス提案を提出 ■ DeFi Unitedは、rsETH回復とAave等の市場正常化を目的とする業界横断の回復枠組みとして、$300M超のETHを確保し、rsETHを段階的に補充する計画を進めた ■ Aave Labsは、2026年5月7日までに攻撃者のEthereum/Arbitrum上の残存rsETH担保ポジションを清算し、担保をDeFi Unitedのウォレットへ移管
Morpho, Euler, ether.fiなど	■ 各DeFiプロトコルにおいては、rsETHへの直接的なエクスポージャーが限定的であったが、LayerZeroのRPC環境等に対する信用懸念から、Morphoにおいては、預入残高が約$1.5B減少	■ Morpho, Euler, ether.fiは関連するブリッジを一時停止 ■ プロトコル同士の被害連鎖を和らげる応急措置として、Fluid, Lido, Ether.fi, 1inchなどが共同で「escape hatch」を構築し、Aaveユーザーの離脱経路を提供
Lido	■ LidoのEarnETH vaultが、Aave上のrsETH/ETHポジションを通じてrsETHに直接エクスポージャーを持っていたため、市場におけるrsETH関連ポジションの巻き戻しや清算によってポジション解消が不利な条件で起こるリスクが発生 ※ Lido Earnとは、Lidoが提供する運用機能で、トークンを受入れ、Aave, Uniswap, Morpho等のDeFi戦略に配分するvaultを指し、EarnETHはそのうちETH・WETH・stETH・wstETH等のETH建てトークンを受入れるvaultを指す	■ EarnETHの新規預入・引出を一時停止。また、DAO資金をLido Earnに配分して損失吸収をするほか、さらに最大2,500stETHを拠出するDAO提案を提出

※各事例に関して公表されている資料及び本報告書の執筆時点で入手可能な情報に基づき調査研究の目的から整理したもので、個別事案に関する責任の所在又は法的評価を示すものではありません

2. 近年の主要な流出インシデントの原因と対策の検討
2.3 事例分析結果に対する考察

署名鍵そのものの窃取を狙った攻撃ではなく、署名に至るシステム・プロセスの脆弱性を突くことでの暗号資産窃取を狙った攻撃手法がとられている

事例分析結果に対する考察（1/4）

攻撃者の狙い	攻撃の共通した特徴と、考えられる防げなかった背景		考察
サードパーティへの侵害（事例①②） マルウェア攻撃（事例③） **署名用トランザクションの改ざんや、署名に至るまでのシステムのプログラム改ざんによって、偽のトランザクションに署名をさせる**	システム開発・運用に関わる人員の権限奪取やマルウェア導入が攻撃の入り口となっている	■ ソーシャルエンジニアリングやフィッシングによる認証情報の漏洩対策が十分に行われていなかった ■ 侵入検知やマルウェア対策が十分に行われておらず不正アクセスを検出できなかった	■ 事例から、署名鍵の流出・窃取のみならず、**署名に至るシステムへの不正侵入や改ざんを想定した対策**の必要性が改めて認識された ■ 暗号資産関連業者がウォレットシステムに外部のサードパーティを利用している場合、署名鍵を預けない場合であっても、**サイバー攻撃対策や本番環境へのアクセス管理、プログラム変更管理等がサードパーティにおいて適切に整備運用されていることが必要**である ■ 攻撃者が不正アクセスの後に本番環境のプログラム改ざんにまで至っている状況を鑑みると、開発者による本番環境アクセスの制御や本番環境で利用するソースコードの管理、本番環境反映に係るビルド／デプロイのプロセスに係るセキュリティ等にも課題があった可能性が推察される。これらの**プログラム変更管理等がサードパーティにおいて適切に整備運用されていることも必要**である ■ 対象とした事例では、電子署名の一部の事案では、暗号資産関連業者は外部評価結果を確認していたが、それのみに依拠せず、外部評価の対象範囲や期間、評価の規準、評価を実施した独立監査人の適格性等を踏まえ、必要に応じて追加的な確認や、相補的な統制を導入する必要があると考えられる ■ 実施時に厳密に取引内容を検証することで、被害を防止できた可能性があった。サードパーティのシステムを利用する場合には、サードパーティの提供するシステムの構造や管理態勢を理解した上で、サードパーティのセキュリティインシデントが自社に及ぼす影響や流出リスクシナリオの分析を行い、**流出を防止するための「自衛策」が何か**を考慮したうえで、署名時の検証プロセスを整備しておくことが重要であったと考えられる
	攻撃者によって、署名トランザクションの改ざんと同時に、本番環境のシステムUIやAPI等のプログラム改ざんまで行われている	■ 本番環境の認証情報や、アクセスの厳格な管理が行われておらず、攻撃者による本番環境のプログラム改ざんを看過した ■ 本番環境に対する不正なプログラムの導入を防止・検知する統制が有効に機能していなかった ■ 未署名トランザクションの改ざんを防止または検知する機構が十分でなかった	
	UIやAPIを改ざんすることにより、不正な取引であることに気づきにくくさせ、署名をさせている	■ ウォレットシステムのUIやAPI改ざん、署名PCのマルウェア感染まで想定した厳格な電子署名の体制・プロセスが設計されていなかったために、署名担当者が取引内容の異常に気付くことができなかった	

※Appendix5. SEAL Certification Framework 参照
※Appendix6. CryptoCurrency Security Standard 参照
※Appendix7. JVCEA 安全管理標準 参照

スマートコントラクトやDeFiの利用には、ロジックの脆弱性や開発者、運営体のガバナンスの不備を考慮する必要がある

事例分析結果に対する考察（2/4）

攻撃者の狙い	攻撃の共通した特徴と、考えられる防げなかった背景		考察
スマートコントラクトの脆弱性を悪用し、スマートコントラクトに保管された暗号資産を直接窃取する	**スマートコントラクトの脆弱性（事例④）** **フラッシュローン攻撃（事例⑤）** 複数のスマートコントラクトを組み合わせた結果生じる脆弱性や、仕様の考慮不足を突いた攻撃が行われている	■ プロトコル全体で発生し得る取引パターンを考慮したバリデーションチェックや、価格・プール等の異常を検知する機構の実装が不十分だった ■ スマートコントラクト監査においてもこのような複数のスマートコントラクトを組み合わせたビジネスロジックの観点での脆弱性が検証対象となっていなかった可能性がある	■ 事例では、スマートコントラクトに十分なバリデーションチェックや異常検知機能があれば被害を防止できた可能性があり、**ロジックの脆弱性が暗号資産の窃取に直接的に繋がる可能性を考慮した、厳重な不正利用防止の機構**が重要であると考えられる ■ 事例では、攻撃者がスマートコントラクトの動作やロジックの脆弱性を理解した上で攻撃を行っているものと考えられ、AIの発達等を背景とした**攻撃者側の脆弱性分析能力の高さ**が推察された ■ スマートコントラクトの**アップグレードを通じたコントロール権の奪取**が複数の事例で攻撃手法として用いられていることから、**暗号資産関連業者がサービスにスマートコントラクトを組み込む場合や、利用するサードパーティがスマートコントラクトを利用している場合には、当該リスクを考慮した対策の導入（権限の分離と高権限に対応する署名鍵の厳格な管理等）が必要**と考えられる ■ また、DeFiプロトコルの利用は、一般的なサードパーティとの契約とは異なり、利用者が全面的にリスクを負う形式となる場合が存在すると考えられるため、利用にあたっては慎重なリスク評価が必要である点にも留意すべきと考えられる
	サードパーティへの侵害（事例①②） **マルウェア攻撃（事例③）** スマートコントラクトのアップグレード機能を悪用し、コントラクトのコントロール権を奪取している	■ 通常の取引とアップグレードを区別せず、同一の署名鍵で実行可能な設計となっていたと考えられる ■ 署名担当者のスマートコントラクトの動作やリスクに関する理解が不十分であったために、取引内容がスマートコントラクトのアップグレードに改ざんされていることを気づけなかった可能性がある	
ラグプル（事例⑥） **詐欺的なプロジェクトに資金を集め、持ち逃げする**	匿名性を利用し、素性を明かすことなくあたかも信頼できるプロジェクトのようにふるまうことで、ユーザーを誤信させる	■ 運営体の身元が明らかでない場合には、運営体の不正を考慮し利用を避ける、または限定的な利用に留める	■ DeFiプロトコルには運営体の身元が明らかでないプロジェクトが存在し、かつ、運営体がコントラクトを自由にアップグレードしたり、プールから資金を移動できる特権を持つ場合が多く、利用する場合には**運営体のガバナンスの不備を考慮する**ことが必要になる

※Appendix4. OWASP SCSVS 参照

署名時においては、トランザクション内容を検証することが求められる。メッセージの可読性が高いウォレット機能導入など、複数の対策を組み合わせて運用することが望ましい

事例分析結果に対する考察（3/4）

サードパーティへの侵害（事例①②） → マルウェア攻撃（事例③） → 権限奪取（事例⑧）

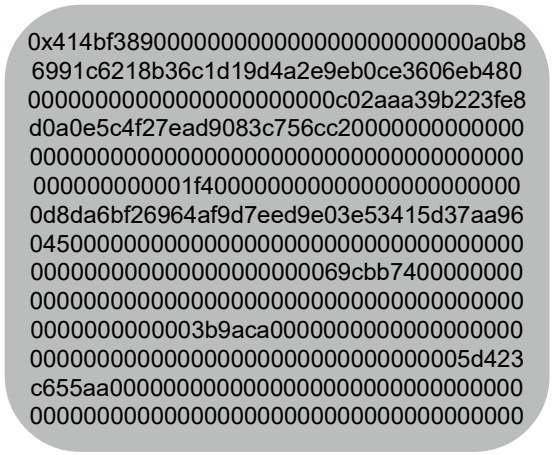
- DeFiやウォレットに関連するスマートコントラクトの更新等における複雑なスマートコントラクト取引では、ウォレットがトランザクション内容を人間が理解しやすい形で表示できず、calldataやEIP-712メッセージが16進数や低レベルな機械可読情報として表示されることがある。特にハードウェアウォレットは画面サイズやUIの制約があるため、複雑な取引内容を十分に分かりやすく表示することに限界もある
- こうしたスマートコントラクトを含む複雑なトランザクションについては、送信先アドレスや送信数量だけではなく、何の操作を行うのか、誰にどの権限が付与されるのか等を署名者が理解した上で署名することが重要である

Clear Signing

- Ethereum Foundationは、ウォレット開発者やセキュリティ企業等とともに、2026年5月12日、トランザクション内容を十分に理解しないまま署名する行為（Blind Signing）の低減を目的として、署名時に「What You See is What You Sign」を実現することを目指す枠組みとして「Clear Signing」を発表
- 中核技術のERC-7730は、スマートコントラクト呼出やEIP-712メッセージ等の構造化データを人間が理解しやすい形で表示するためのJSON形式の記述子（descriptor）標準。ドラフトERCとして2024年2月に提案されて以降エコシステム横断的な標準として発展し、v2ではクロスチェーン取引やソフトウェアウォレットを含む、より幅広いユースケースへの対応が拡張されている。
- 記述子を配布する中立的でミラー可能なレジストリ、記述子の正確性について独立したレビュー・アテステーションを可能にする仕組み及びウォレット・プロトコル開発者向けの導入ツールを含む総合的な仕組みとして設計される
- ブリッジ/クロスチェーン取引、ステーキング、権限付与、スマートコントラクトのアップグレード・管理等の複雑な取引において、署名前の内容確認が不十分であることに起因する資産流出リスクの低減策として有効
- 一方、Clear Signingの効果は、その表示内容の正確性や記述の真正性、そしてウォレットが採用する信頼モデルに依存する。誤った記述子や改ざんされた供給経路を信頼すれば、誤認を招く表示が生じ得るため、表示内容を無条件に安全とみなすべきではないことに留意が必要。承認のダブルチェック、マルウェア対策、外部委託先管理、権限分離、異常検知等の対策と組み合わせて運用することが望ましい

＜イメージ＞

calldata



Clear Signing	
Action	Swap
Send	1.000USDC
Receive min.	0.42WETH
Protocol	Uniswap V3
Network	Ethereum
…	

DeFiの資産流出の要因は、CI/CD・クラウド・署名権限・クロスチェーン検証等、チェーン外での統制不備に関するものであり、CEXを含む暗号資産関連業務全般に共通するリスクである

事例分析結果に対する考察（4/4）

攻撃者の狙い	攻撃の共通した特徴と、考えられる防げなかった背景		考察
署名鍵やスマートコントラクトの脆弱性でなく、CI/CD、クラウドIAM/KMS、管理者権限等、周辺インフラや運用プロセスを侵害し、DeFiプロトコル上の発行・担保・出金・クロスチェーン検証の前提を崩すことで、資産を窃取する	GitHub、CI/CD、クラウドIAM/KMS、署名プロセス等を含むオフチェーン領域の侵害を起点としていた	■ サプライチェーンも含めたシステム全体としての統制・評価が十分でなかった可能性がある	■ DeFiプロトコルの安全性をスマートコントラクト監査の有無だけで判断することは不十分であり、**GitHub、CI/CD、クラウドIAM/KMS、署名サービス、オラクル、RPC、外部協力者管理、チェーン最終性まで含めた統合的なリスク評価が必要**であることを示している ■ 高権限操作については、単なるマルチシグではなく、**権限分離、閾値強化、タイムロック、移転先allowlist、二者承認、署名内容のデコード確認、署名対象の取引コンテキスト検証を組み合わせる必要**がある。特に**admin移転、KMS policy変更、担保市場追加、オラクル変更、発行上限変更、出金上限変更は、通常送金とは異なる高リスク操作として扱うべき**である ■ クロスチェーン・ブリッジ等を利用する場合は、単一RPC等への依存を避け、**複数ソース検証、最終性リスクに応じた確認数設定、遅延決済、サーキットブレーカー、発行量・担保価値の不変条件監視を導入することが重要**である ■ 問題の本質は、権限管理、認証情報管理、CI/CD、クラウド設定、署名統制、委託先管理、プログラム変更管理、クロスチェーン接続管理等の不備に起因しており、**CEX、カストディアン、ウォレット事業者等の中央集権型サービスにおいても同様に成立し得るリスク**である ■ 特に、GitHub・CI/CD・クラウドIAM/KMS・署名サービス等のオフチェーン領域への侵害は、暗号資産交換業者等においても、ホットウォレット管理、送金承認、鍵管理基盤、API基盤、資産移動管理等へ波及し得るため、DeFi固有の問題として限定的に捉えるべきではない。また、ブラインド署名、署名内容確認不足、管理権限への過度な集中、外部サービスへの依存、異常時の自動停止不足等についても、CEX等における出庫承認、資産移動、ウォレット更新、外部カストディ接続等の業務に共通するリスクであり、**DeFi・CeFiを問わず多層的統制が必要**である ■ また、中央集権型サービス提供者がDeFiインフラやプロトコルを利用・接続する場合、**委託先・外部サービスとしての統制確認**に加え、**当該外部サービスの障害・侵害・仕様変更が自社資産や顧客資産に与える波及リスクをシナリオベースで評価**し、**自社側で取り得る上限設定、停止条件、監視、追加承認等の自衛策を整備する必要**がある
	ブラインド署名、事前署名等、人間による署名・承認行為そのものを攻撃経路として悪用していた	■ 署名対象の実質的な内容を確認できる仕組みや運用、署名者教育等、人的統制や署名統制が十分ではなかった可能性がある	
	admin権限、署名権限、ミント権限、リスクパラメータ権限等の高権限操作を悪用していた	■ 権限分離、多者承認、タイムロック、変更上限、変更先制限等の高リスク操作に対する統制が不十分だった可能性がある	
	クロスチェーン検証やチェーン最終性等の外部依存要素への信頼を前提とした構造を悪用し、虚偽データや無効チェーン上の取引を正当なものとして処理させていた	■ 単一RPC等への依存、複数ソース検証不足、reorg耐性設計不足、異常検知不足等、外部依存リスクを前提とした設計・監視が十分ではなかった可能性がある	
	攻撃実行後も、不正ミントや出金が継続し、攻撃者は短期間で複数回の取引を連続実行していた	■ 異常取引検知、経済的不変条件の監視、サーキットブレーカー、自動停止等のリアルタイム監視や抑止機能が不十分だった可能性がある	

3. 暗号資産関連業者の運営に資する提言

3.1 導出された対策とガイドラインの比較分析

機能別整理及び事例分析から導出された攻撃手法・考えられる対策と、各ガイドライン等の比較を行う

対策とガイドラインの比較

暗号資産事業に関連する各機能に対して想定される攻撃手法

暗号資産関連事業が自ら統制するまたは外部委託先管理として統制する範囲と考えられる機能について、MITRE等を参考に想定される攻撃手法を整理

- CEX
- HWウォレット
- SWウォレット
- MPC／鍵管理インフラ
- 物理基盤インフラ
  （クラウド／HSM／ソフトウェア供給源等）

事例分析から理解した実際に流出に至った攻撃手法

2023年以降の被害額が大きいインシデントについて攻撃の手法を分析し、手口に利用された脆弱性を整理

- サードパーティへの侵害
- スマートコントラクトの脆弱性
- ラグプル（資金持ち逃げ）
- フラッシュローン攻撃
- マルウェア攻撃

攻撃手法に対し考えられるセキュリティ対策

攻撃手法・脆弱性に対して考えられるセキュリティ対策を検討、例示

（主要な対策項目）

- 秘密鍵の流出リスク対策
- 不正なトランザクションの検知・防止
- フィッシング・マルウェア対策
- アクセス制御
- プログラム管理
- サプライチェーン攻撃

等

ガイドライン等との比較

本研究調査で確認対象としたガイドライン等との比較

（ガイドライン等）

- NIST CSF 2.0
- 金融庁事務ガイドライン
- 金融庁サイバーセキュリティガイドライン
- FISC 安全対策基準
- MITRE ATT&CK
- MITRE AADAPT
- JVCEA暗号資産安全管理標準
- OWASP／SCSVS

等

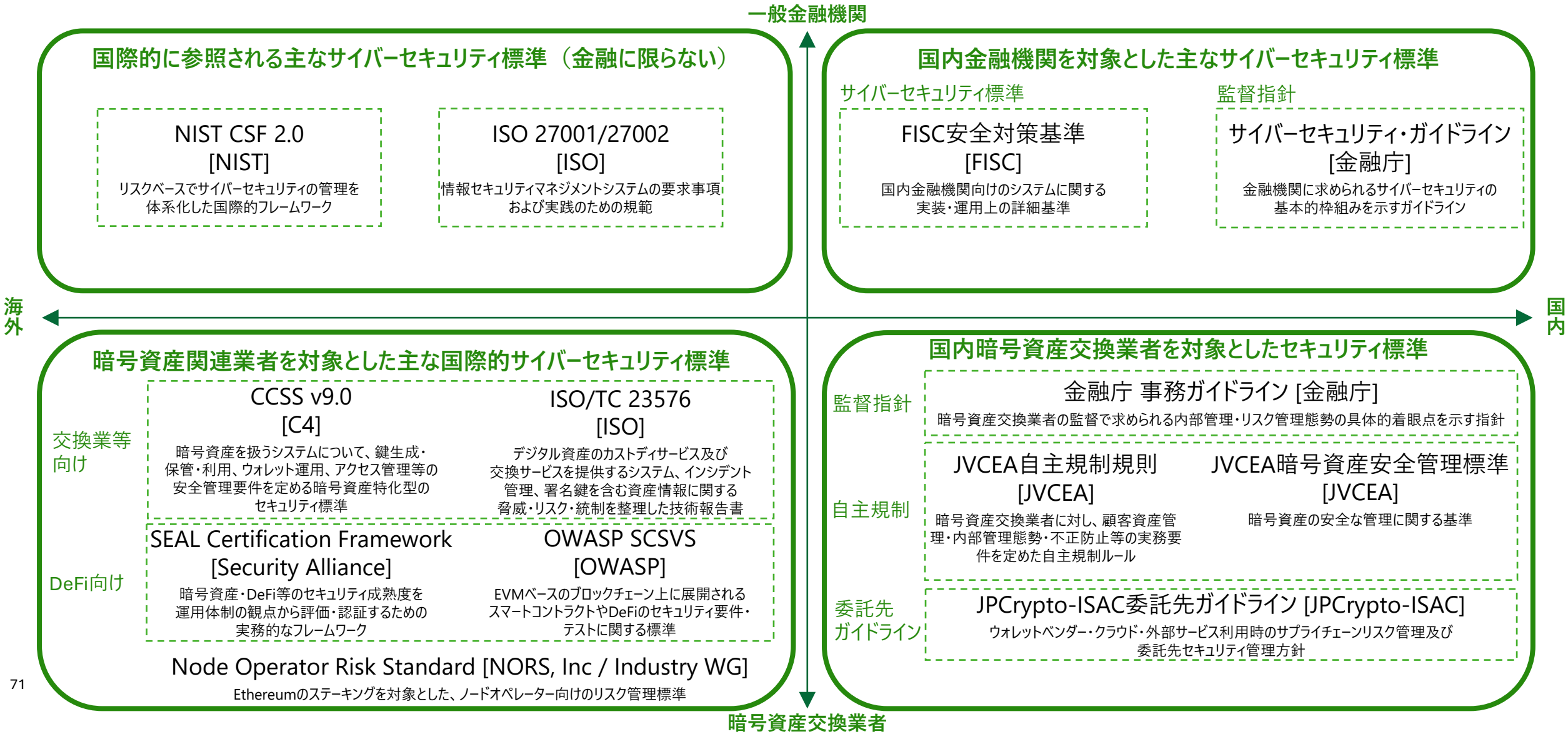
本研究で参照したガイドライン・脅威分析フレームワークの一覧

参照したガイドライン・脅威分析フレームワーク	正式名称	発行日／版	発行元	概要
NIST CSF 2.0	Framework for Improving Critical Infrastructure Cybersecurity	2024.2.26 ／Version 2.0	米国国立標準技術研究所（NIST）	リスクベースでサイバーセキュリティの管理を体系化した国際的フレームワーク
ISO/IEC 27001	-	2022.10 ／Edition3	国際標準化機構（ISO）／国際電気標準会議（IEC）	情報セキュリティマネジメントシステム（ISMS）の要求事項を定める国際規格。組織が情報セキュリティリスクを識別・評価・管理し、継続的に改善するための枠組み。認証取得の基準として用いられる。
金融庁サイバーセキュリティガイドライン	金融分野におけるサイバーセキュリティに関するガイドライン	2024.10.4	金融庁（FSA）	金融機関に求められるサイバーセキュリティの基本的枠組みを示すガイドライン
FISC 安全対策基準	金融機関等コンピュータシステムの安全対策基準・解説書	2026.3.25 ／第14版	一般社団法人金融情報システムセンター（FISC）	国内金融機関向けのシステムリスクに関する詳細な実装基準
JVCEA 自主規制規則	暗号資産交換業者に関する自主規制規則	–	日本暗号資産取引業協会（JVCEA）	暗号資産交換業者に対し、顧客資産管理・内部管理体制・不正防止等の実務要件を定めた自主規制ルール
JVCEA 暗号資産安全管理標準	暗号資産安全管理標準	2025.6	日本暗号資産取引業協会（JVCEA）	暗号資産の安全な管理に関する標準
金融庁事務ガイドライン	第三分冊：金融会社関係 16.暗号資産交換業者関係	2025.4.1	金融庁（FSA）	暗号資産交換業者の監督において求められる内部管理・リスク管理態勢の具体的着眼点を示す指針
JPCrypto-ISAC 委託先ガイドライン	暗号資産関連事業者における委託先管理ガイドライン	2026.1.26	一般社団法人JPCrypto-ISAC	ウォレットベンダー・クラウド・外部サービス利用時のサプライチェーンリスク管理および委託先セキュリティ管理指針
OWASP SCSVS	Smart Contract Security Verification Standard	2024	Open Web Application Security Project（OWASP）	主にSolidityで記述され、EVMベースのブロックチェーン上に展開されるスマートコントラクトやDeFiのセキュリティ要件やテストに関する標準

本研究で参照したガイドライン・脅威分析フレームワークの一覧

参照したガイドライン・脅威分析フレームワーク	正式名称	発行日／版	発行元	概要
CCSS v9.0	CryptoCurrency Security Standard v9.0	2024.12.17	CryptoCurrency Certification Consortium (C4)	暗号資産を扱うシステムについて、鍵生成・保管・利用、ウォレット運用、アクセス管理、監査証跡等の安全管理要件を定める暗号資産特化型のセキュリティ基準
SEAL Certification Framework		–	Security Alliance (SEAL)	暗号資産・DeFiプロジェクト等のセキュリティ成熟度を、運用体制の観点から評価・認証するための実務的なフレームワーク
MITRE ATT&CK	MITRE ATT&CK Framework	2025.10.28 ／v18.1	MITRE Corporation	システムに対する攻撃者の戦術と技法を、実世界の観測に基づき体系化した包括的なフレームワーク
MITRE AADAPT	MITRE AADAPT Framework	2025.7.14	MITRE Corporation	暗号資産等のデジタル資産管理システムにおける攻撃者の戦術と技法を体系化した包括的なフレームワーク
MITRE D3FEND	MITRE D3FEND Framework	2025.12.16 ／v1.3.0	MITRE Corporation	サイバー攻撃に対する防御技術・対策を体系化したナレッジベース。MITRE ATT&CKと対応付け、防御手法の設計・評価を支援する
ISO/TC 23576	Blockchain and distributed ledger technologies — Security management of digital asset custodians	2020.12 / Technical Report	International Organization for Standardization（ISO）	デジタル資産のカストディサービスおよび交換サービスを提供するシステム、インシデント管理、署名鍵を含む資産情報に関する脅威・リスク・統制を整理した技術報告書
NORS	Node Operator Risk Standard	2024.8 / Certification framework	NORS, Inc. / industry working group	Ethereumのステーキングを対象とした、ノードオペレーター向けのリスク管理基準

本研究で参照したガイドラインの一覧（関係図）



対応すると考えられる項目はガイドライン等に存在しており、事業者においては、自社が講じるべき対策を具体化・深堀することが求められる。

事例分析から抽出された脆弱性とガイドライン等の対応関係（1/2）

事例から抽出された脆弱性	事例	考えられるセキュリティ対策例	ガイドライン(*1)に示された対策例
フィッシング対策が不十分 (*2)	①、③	■事例に基づくフィッシング対策の教育 ■定期的な注意喚起と確認	➢ 個人への意識向上とトレーニングを提供（NIST／PR.AT-02） ➢ サードパーティ担当者の教育・研修の受講（金融庁／2.3.2.②） ➢ サイバーセキュリティ、ソーシャルエンジニアリングの教育（FISC／統14）
マルウェア攻撃対策が不十分 (*2)	①、③	■シグニチャベースの対策ソフトに加え、振る舞い検知機能のマルウェア対策ソフトやEDRの導入・監視	➢ ソフトウェアやデータの監視を行う（NIST／DE.CM-09） ➢ システムをマルウェア感染から保護する（金融庁／2.3.4.1.④） ➢ 不正プログラムへの防御・検知策を講じる（FISC／実20、実21）
不正アクセス対策が不十分 (*2)	①、②、③	■ネットワークの論理的・物理的分離やセグメントを細分化する ■本番環境へのアクセス権の厳格な管理	➢ ネットワークが未認可のアクセスから保護されている（NIST／PR.IR-01） ➢ ネットワークの物理的な分離、セグメントの細分化（金融庁／2.3.4.4.①,c） ➢ 外部ネットワークからアクセス可能な接続機器を制限する（FISC／実15）
不正なプログラムへの差し替えやAPIの改ざん	①、②、③	■本番環境のプログラム変更の防止 ■変更管理の遵守・コードスキャン実施、ログ監視	➢ セキュアなソフトウェア開発プラクティスの実行と監視（NIST／PR.PS-06） ➢ 開発環境等と本番環境との分離、不正な変更防止（金融庁／2.3.4.4.b） ➢ システム開発・変更における確認・検証手順の明確化（FISC／実75）
署名用トランザクションファイルの改ざん	①、②、③	■署名用トランザクションの改ざんを防止・検知する技術的措置	➢ トランザクション署名における意図しないデータの混入の防止（JVCEA標準）
ブラインド署名	①、②、③、⑧	■メッセージの可読性が高いウォレット機能の導入 ■サイバー攻撃を想定した署名担当者の教育・研修	➢ 移転先、対象資産・数量の適切性の確認（JVCEA標準） ➢ 署名済みトランザクションデータの内容の検証（JVCEA標準）
同一ウォレットでの資産集中管理	①、②、③、④、⑤	■単位時間当たりの送金額の検知・制限 ■複数ウォレットへの分散化	➢ ウォレット分散等の流出リスクを低減するための措置（JVCEA規則／第20条） ➢ 流出等のリスクに応じた暗号資産の移転に係る上限額の設定（JVCEA規則／第26条）
スマートコントラクトのアップグレード機能を悪用した権限の奪取	①、②、③	■操作内容毎の権限の分離とアップグレード権限の厳重な管理	➢ セキュアなソフトウェア開発プラクティスの実行と監視（NIST／PR.PS-06） ➢ 変更に伴うリスクのインパクトがアセスメントされている（NIST／ID.RA-07） ➢ セキュリティ・バイ・デザインの実施（金融庁／2.3.4.3.①） ➢ セキュリティ・バイ・デザインを含むシステム開発・変更手順の整備（FISC／実75） ➢ ユニットテスト、統合テスト、セキュリティテストを含む包括的なテストカバレッジ（OWASP SCSVS／S3） ➢ ロールベースアクセス管理（RBAC）の導入（OWASP SCSVS／S4） ➢ Multisig Ops（SEAL Certification Framework）
コントラクトにおける異常な取引を防止する機構の導入が不十分	④、⑤	■コントラクトの機能の追加や組合せによって生じるシステム全体としての脆弱性を考慮した機能検証と、異常な取引を防止するチェック機能等の導入	

(*1):引用したガイドラインは、次のものを指す。「NIST」：NIST CSF 2.0、「金融庁」：金融分野におけるサイバーセキュリティに関するガイドライン、「FISC」：金融機関等コンピュータシステムの安全対策基準・解説書（第13版）、「JVCEA規則」：暗号資産交換業に係る利用者財産の管理等に関する規則、「JVCEA標準」：暗号資産安全管理標準、「OWASP SCSVS」： OWASP Smart Contract Security Verification Standard

(*2): 根拠となる情報は得ていないものの、実施されていなかった可能性があるものとして記載した

対応すると考えられる項目はガイドライン等に存在しており、事業者においては、自社が講じるべき対策を具体化・深堀することが求められる。

事例分析から抽出された脆弱性とガイドライン等の対応関係（2/2）

事例から抽出された脆弱性	事例	考えられるセキュリティ対策例	ガイドライン(*1)に示された対策例
外部協力者権限の過大付与 資格情報の失効・棚卸不足 CI・クラウドへの横展開可能性	⑦、⑩	■最小権限化、JITアクセス、資格情報の短命化、定期棚卸し、委託先管理強化	➢ アクセス権限の最小化・定期レビュー（NIST／PR.AA-05） ➢ ID・資格情報の管理（NIST／PR.AA-01） ➢ CI/CD・クラウド設定変更管理（NIST／PR.PS-01） ➢ 第三者リスクの継続的な評価・監視（NIST／GV.SC-07） ➢ アクセス制御・認証の強化（OWASP SCSVS／SCSVS-AUTH） ➢ セキュアな開発・テスト・デプロイ（OWASP SCSVS／SCSVS-CODE） ➢ CI／CD・クラウド・サプライチェーン統制（SEAL／DevOps & Infrastructure） ➢ アカウント棚卸し・資格情報管理（SEAL／Identity & Accounts） ➢ 鍵管理・権限付与取消・最小権限（CCSS／1.04.1・2・3, 1.05.1・3, 1.06.2）
CI/CD認証情報保護不足 クラウドAPI・KMS権限制御不備	⑦	■Workflow変更監視・強制レビュー ■CI/CDから署名操作遮断 ■KMSポリシー変更の多者承認	
権限分離不足 閾値不足 タイムロック未設定 変更制限なし	⑦、⑧、⑩	■閾値強化（3 of 5等） ■タイムロック ■変更先allowlist ■変更倍率制限	➢ ガバナンス・ビジネスロジック保護（OWASP SCSVS／SCSVS-GOV） ➢ マルチシグ・タイムロック・鍵ローテーション（OWASP SCWE／SCWE-155） ➢ マルチシグ運用・閾値管理（SEAL／Multisig Ops）
外部依存 Reorg耐性不足	⑧、⑨、⑩	■複数ソース検証 ■遅延決済 ■不整合検知	➢ 外部データフローの把握・管理（NIST／ID.AM-03） ➢ 外部サービスの継続的監視（NIST／DE.CM-06） ➢ 不整合・異常イベントの分析（NIST／DE.AE-02、DE.AE-03） ➢ オラクル・外部データ検証（OWASP SCSVS／SCSVS-ORACLE） ➢ ブリッジ・状態管理の完全性確保（OWASP SCSVS／SCSVS-BRIDGE） ➢ DeFi固有リスク・経済的不変条件の検証（OWASP SCSVS／SCSVS-DEFI） ➢ 緊急停止・サーキットブレーカー（OWASP SCWE／SCWE-156） ➢ 監視・対応プレイブック・訓練（SEAL／Incident Response） ➢ DeFiリスク管理・取引監視（SEAL／Treasury Ops） ➢ トレジャリー運用・DeFiリスク管理・取引監視（SEAL／Treasury Ops） ➢ 署名鍵等を取り扱うカストディアンおよびサービス事業者のシステム評価（ISO/TR 23576） ➢ Ethereumのステーキング事業者およびノードオペレーターの評価（NORS／Risk & Control Matrix）
リアルタイム監視・ 異常抑止機能の不足	⑦、⑧、⑨、⑩	■経済的不変条件監視 ■異常出金検知 ■自動停止 ■発行上限・出金上限	

(*1):引用したガイドラインは、次のものを指す。「NIST」：NIST CSF 2.0、「金融庁」：金融分野におけるサイバーセキュリティに関するガイドライン、「FISC」：金融機関等コンピュータシステムの安全対策基準・解説書（第13版）、「JVCEA規則」：暗号資産交換業に係る利用者財産の管理等に関する規則、「JVCEA標準」：暗号資産安全管理標準、「OWASP SCSVS」： OWASP Smart Contract Security Verification Standard、「ISO/TR 23576」：Blockchain and distributed ledger technologies — Security management of digital asset custodians、「NORS」： Node Operator Risk Standard

3. 暗号資産関連業者の運営に資する提言

3.2 暗号資産関連業者の運営に資する提言（案）

暗号資産の出庫や署名などの重要業務を外部サービスに依存する場合、再委託先を含む統制の実効性を委託元が自ら検証できる管理態勢を構築する必要がある

分析や事例から導出された提言（案）（1/5）

委託先管理の高度化

■ 暗号資産関連業者には、**サプライチェーンにおける機能間の相互関連性を明らかにした上で、提供するサービスに影響を及ぼすリスクを分析する**ことが求められるか。こうしたリスクは、単に「第三者の脆弱性」として扱うのではなく、未検証の外部依存として再整理し、独立検証、最小権限、継続的監視、異常検知及び自動停止等のゼロトラスト型統制を適用することが望ましい。特に、暗号資産の送金や署名といった重要業務を外部サービスに依存する場合、委託先の侵害が自社の資産流出に直結し得ることを前提に、委託先管理を高度化する必要がある。今回分析した事例においても、委託先・外部協力者・外部インフラの侵害や設定不備が、トランザクション改ざん、署名権限奪取、不正ミント、クロスチェーン検証の破綻等に繋がっている

■ 具体的には、**委託先のフィッシング・マルウェア対策、本番環境アクセス管理、CI/CD管理、クラウドIAM・KMS管理、プログラム変更管理、ログ監視等の多層的なサイバーセキュリティ管理状況を定期的に評価**するとともに、再委託先を含めたアクセス権限の最小化、JIT化、資格権限の短命化、定期棚卸し、プロジェクト終了時の即時失効などが必要となるか

■ そのためには、委託先に対する定期監査および継続的モニタリングの実施等を通じて、**再委託先を含む統制の実効性を委託元が自ら検証できる管理態勢を構築**するとともに、検証に必要な事項（監査受入れ、報告義務、認証情報管理、違反時の是正措置、ログ保全、再委託の管理義務等）を委託契約に反映し、**委託先が提供するサービス・システムの構造について適切にデューディリジェンスすること**等が必要と考えられる。評価の結果が不十分な場合には、追加的な自衛策、利用範囲の制限、代替委託先の検討、委託関係の見直しも含めて判断する必要があるか

■ また、攻撃者が自社または委託先のITシステム関連要員を介して重要システムへのアクセス権限を不正取得するリスクを踏まえ、CCSS等を参考に**委託先その他の外部関係者に関する管理体制を構築すること**が不可欠か。具体的には、本人確認、法令上認められる範囲でのバックグラウンドチェック、セキュリティ教育、定期的なアクセス権限レビュー等の実施状況を確認することが考えられるか

※なお、提言は一般的な参考情報であり、ここに記載の提言のみに対応すれば足りるものでなく、各組織の実態やリスクに応じた追加の検討・対策が必要であることに留意されたい

暗号資産の出庫や署名などの重要業務については、不正アクセスによるプログラム改ざんまで想定した管理策の充実強化が必要である

分析や事例から導出された提言（案）（2/5）

不正プログラムの混入・改ざん防止策

■ 不正プログラムの混入・改ざんにより、署名に至るまでのUI、API、CI/CD、クラウド環境、未署名トランザクション生成ロジックが改ざんされる事例が多く見られた。例えば、Bybit事案ではウォレットUIのJavaScript改ざん、SwissBorg事案ではAPIロジック改ざん、Radiant事案ではマルウェアによるトランザクション改ざん、Resolv事案ではGitHub workflowを悪用した認証情報窃取が確認されており、いずれも正規の署名プロセスを悪用する攻撃であった

■ 具体的な対応としては、**本番環境認証情報の厳格管理、厳格なCI/CDの強制レビュー、ソフトウェア部品表（SBOM）の整備・更新、ソースコードやファイルの完全性検証、APIレスポンスのバリデーション、運用監視による改ざんや異常挙動を早期に検知し即応する体制の構築**等が考えられるか。また、署名プロセス、KMS、CI/CD、クラウドIAM及び本番環境に関する特権操作について、ネットワーク分離、職務分離、ハードウェアに基づく認証情報、短期認証、期限付きのJIT権限昇格、恒久的管理者アクセスの排除、ならびにKMSポリシー変更等の高リスク変更に対する複数者承認を実装することが望ましい。加えて、**CI/CD環境や開発者端末から署名操作・KMS操作・本番環境高権限操作へ直接到達できないよう、ネットワーク分離、権限分離、短命認証、KMSポリシー変更の多者承認を導入**すべきか。また、外部ライブラリの取り込み等においては、汚染されたライブラリの取り込みによって社内システムへ汚染が広がることを防ぐため、バージョン固定や自動実行禁止などの基準を明確にすることも有効と考えられる。

■ また、**ウォレット操作端末についても、EDR、振る舞い検知、マルウェア対策、専用端末化、外部ファイル実行制限、通信監視を組み合わせることで、署名直前の改ざんリスクを低減する必要**があるか。これとは別に、ウォレット、署名、CI/CD、スマートコントラクト及びクラウド制御に関するコンポーネントのビルド・デプロイ環境は、本番環境への適用前に完全性確認及び変更承認を行うことを前提として、分離され、監査可能であり、可能な範囲で外部アクセスを制限しつつ再現可能性を確保することが必要か。

※なお、提言は一般的な参考情報であり、ここに記載の提言のみに対応すれば足りるものでなく、各組織の実態やリスクに応じた追加の検討・対策が必要であることに留意されたい

暗号資産の不正送金防止に関する措置として多層的な予防統制を導入することに加えて、厳格な署名時の検証が不可欠である

分析や事例から導出された提言（案）（3/5）

暗号資産の不正送金防止に関する措置

■ 暗号資産関連業者は、暗号資産の不正送金を防止するためには、単にマルチシグやハードウェアウォレットを導入するだけでは不十分であり、取引の目的及び承認済みポリシーに基づく署名を徹底するため、**送金トランザクションに関する多層的な統制を要件として具体的に検討し導入**することが不可欠か

■ Bybit、SwissBorg、Radiant事案では、署名者が画面上では正常に見える取引に署名した結果、不正な権限変更や資金流出が発生している。送金トランザクション（特に、DeFiやウォレットに関連するスマートコントラクトの更新等における複雑なスマートコントラクト取引）については、**金額・頻度・新規宛先・未知コントラクト・権限変更・大口出金等に応じた追加承認、遅延実行、オフライン署名、シミュレーション、デコード結果の技術者レビュー、Clear Signing等による可読性向上等、複数の対策を組み合わせて運用**することが望ましい.。また、取引データ又は承認画面が外部API又はウォレットインフラを通じて生成される場合には、署名前に取引内容又はポリシー適合性を暗号学的に検証できる仕組み等も検討され得る。

■ さらに、**複数ウォレット運用、アドレスごとの資産上限、出金上限、発行上限、異常出金検知、経済的不変条件監視、自動停止・サーキットブレーカーにより、仮に一部統制が突破された場合でも被害を限定する設計**が必要か。署名時の取引内容の検証にあたっては、不正またはミスを防止するための相互牽制に加えて、**取引内容の妥当性が判断できるための検証方法や検証担当者の適格性・バックグラウンド等についても考慮**するほか、検証担当者のトレーニングを行うことが望ましい

■ また、一度に大量の暗号資産が流出するリスクを想定し、**複数ウォレットの使い分けやアドレスごとの資産保有の上限設定により残高集中を回避**すること等も考慮すべきか

■ 加えて、自社および業界団体で内外の流出事案を収集・分析・共有・点検することや、小規模事案のパターン観測から新たな攻撃手法やトレンドを早期に把握して統制に反映することも、不正送金の未然防止に有益か

※なお、提言は一般的な参考情報であり、ここに記載の提言のみに対応すれば足りるものでなく、各組織の実態やリスクに応じた追加の検討・対策が必要であることに留意されたい

暗号資産関連業者は、スマートコントラクトやDeFiの利用の拡大に備えた対策の整理を検討する必要がある

分析や事例から導出された提言（案）（4/5）

スマートコントラクトやDeFiへの対応

■ スマートコントラクトやDeFiについては、**コード単体の脆弱性を確認するのみでは十分ではない**。デプロイ後の管理者権限、アップグレード権限、ミント権限、オラクル設定、リスクパラメータ、出金上限、クロスチェーン設定等の運用によって、プロトコルの実質的なリスクは変化し得る。このため、中央集権型の暗号資産関連業者における署名鍵管理やトランザクション真正性の担保のためのオペレーションと同様に、スマートコントラクトやDeFiにおいても、**権限管理、変更管理、監視、異常時停止等のオペレーション統制が必要**となるか

■ Balancer v2やEuler事案では、スマートコントラクトのロジックや機能追加・組み合わせに起因する脆弱性が悪用された一方、Drift, Litecoin/Near Intents, Kelp/LayerZero事案では、管理権限、オラクル、ブロックチェーンのreorg耐性、単一障害点への依存、発行権限、クロスチェーン検証等といった運用・構成面の不備が被害に繋がっている。これらは、**コードレビューやスマートコントラクト監査のみならず、権限設計、変更管理、監視、異常時停止、外部依存先管理を含む、実運用を前提とした統制の必要性**を示している

■ 具体的には、**スマートコントラクトの設計・実装・変更に係る技術的検証に加え、管理権限の行使に係る統制を整備することが不可欠**か。特に、ミント、burn、lock/unlock、担保追加、オラクル変更、risk parameter変更、出金上限変更、admin移転、コントラクトアップグレード等の高リスク操作については、権限分離、多者承認、タイムロック、変更先allowlist、変更倍率制限、初期上限、段階的引上げ、自動停止を組み合わせることが望ましい

■ また、DeFiやクロスチェーン領域では、外部オラクル、RPC、ブリッジ、他プロトコル等への依存がリスク要因となるため、これらの**外部依存関係を含めたリスク管理が必要**となるか。具体的には、複数オラクル、最低流動性・保有分散・取引期間要件、異常価格の自動拒否、複数ソース検証、reorgリスクに応じた入金確定条件の設定、遅延決済、スワップ上限、クロスチェーン検証・外部データ取得経路の冗長化、単一の検証主体・データソースへの依存回避、発行量・担保価値の不変条件監視等を整備することが考えられる

■ このように、スマートコントラクトやDeFiのリスク低減においては、コードの脆弱性を監査で確認することに加え、管理権限や署名権限の設計、変更承認、パラメータ変更、外部依存先、監視・検知、緊急停止を含む**オペレーション全体を統制することが不可欠**か。スマートコントラクト監査を受けている場合であっても、監査対象外の関数、後続アップグレード、外部依存、運用権限、クロスチェーン構成がリスクとして残り得るため、**監査結果のみに依拠せず、継続的な運用管理と補完的な統制を組み合わせる**ことが望ましい

※なお、提言は一般的な参考情報であり、ここに記載の提言のみに対応すれば足りるものでなく、各組織の実態やリスクに応じた追加の検討・対策が必要であることに留意されたい

外部評価は有効な手段である一方、その対象・限界を確認し、自社リスクに応じた追加確認や補完統制と組み合わせる必要がある

分析や事例から導出された提言（案）（5/5）

外部評価の活用

■ 暗号資産関連業者は、ウォレットプロバイダー、ステーキングサービスプロバイダー、DeFiプロトコル、ブリッジ、スマートコントラクト、クラウドサービス、CI/CD環境、および署名サービスを含む外部サービスプロバイダーについて、**独立した第三者評価を活用することが必要か**。重要な業務を支えるインフラ提供者については、そのような評価を利用して、最低限の保証水準が確保されていることを確認すべきか（例：SOC 2 または ISO/IEC 27001 の認証・保証報告書、脆弱性評価、ペネトレーションテスト、完了したコード監査の証跡、該当する場合のスマートコントラクト監査、および鍵管理・署名アーキテクチャに関する文書）。ただし、第三者評価は万能ではなく、その結果を利用する際には、評価の対象範囲、実施時期、手法、前提条件、除外事項、是正措置の実施状況、ならびに評価実施者の独立性および専門性・適格性を確認した上で活用することが必要か

■ 事例では、スマートコントラクト監査や第三者保証が存在していた場合でも、監査対象外のコンポーネント、後から追加された機能、外部サービスとの連携部分、外部データ取得経路、クロスチェーン検証の仕組み、開発・リリースプロセス、クラウド上の権限管理、鍵管理、署名関連サービス等の周辺統制が十分に評価されていない可能性が示されている。そのため、外部評価結果を確認する際には、「何が評価されているか」だけでなく、「**何が評価されていないか」を把握し、自社の流出リスクシナリオに照らして不足部分を補完する**ことが必要か

■ また、外部評価を受けていること自体を安全性の根拠とするのではなく、評価結果の指摘事項、是正状況、再評価の有無、監査後の変更管理、委託先の運用実態まで確認することが望ましい。必要に応じて、委託先監査、追加質問票、技術的証跡の確認、オンサイトレビュー、継続的モニタリング、自社側の補完統制を組み合わせるべきか

※なお、提言は一般的な参考情報であり、ここに記載の提言のみに対応すれば足りるものでなく、各組織の実態やリスクに応じた追加の検討・対策が必要であることに留意されたい

3. 暗号資産関連業者の運営に資する提言
3.3 その他の検討事項（案）

匿名性・越境性・即時性を有する暗号資産リスクに対応するため、情報共有機関を中心とした業界横断・国際連携型の情報共有・分析機能の高度化が求められる

提言：情報共有機関を中心とした業界横断・国際連携型の情報共有・分析機能の強化

課題

- ■ 暗号資産取引は匿名性・越境性・即時性を特徴とし、それを突く攻撃手法は高度化している
- ■ そのため、攻撃情報・脆弱性情報・不正ウォレット・凍結要請・インシデント対応知見等は、事業者間での共有がより重要となる
- ■ この構造の下では、各事業者の内部管理のみでは、リアルタイムの検知・追跡・凍結・被害拡大防止に限界がある

提言

■ **構想についての提言**

上記構造的な課題を抜本的に解決するためには、例えば、以下の取組みが国際的に進展することが望まれる

1. 共通データ項目・共通フォーマットの整備

ウォレット、トランザクション、リスク属性、凍結要請、攻撃パターン、脆弱性情報等を国際的に共有可能な形式で標準化する

2. 情報共有機関（JPCrypto-ISACなど）を中心とした情報共有・分析機能の強化

- ➢ 情報共有機関が、脅威情報やインシデント情報を集約・分析し、会員に対する注意喚起、対応例の共有、演習・訓練、委託先管理に関する実務知見の蓄積を担う
- ➢ 情報共有機関が、国内事業者間の情報共有に加え、海外ISAC等との連携を通じて、国際的な情報共有・分析機能を担う

3. 継続的な知見更新と実務への反映

- ➢ 小規模事案や未遂事案を含む攻撃パターンを継続的に収集・分析し、得られた知見をガイドライン、委託先管理、署名・出金統制、訓練シナリオ等に反映する

■ **実現に向けた提言**

民間で多様な取組みが進む中、個別事業者の対応にとどまらず、JPCrypto-ISAC等の情報共有機関が、脅威情報、脆弱性情報、不正ウォレット情報、インシデント対応知見等を集約・分析し、事業者間で迅速に共有できる枠組みを強化することが望まれる。そのためには、共通データ項目・共有フォーマットの整備、海外ISAC等との連携、演習・訓練や委託先管理に関する実務知見の蓄積を進め、各事業者が得られた知見をガイドライン、署名・出金統制、委託先管理、訓練シナリオ等に継続的に反映する仕組みを構築することが重要か。

AIの進展を踏まえ、アタックサーフェスの削減、重要システムの分離、教育・訓練、脆弱性情報開示制度の見直しを含む、技術・運用一体の対策が急務となっている

提言：AI時代の暗号資産サイバーセキュリティ対策

課題

- AnthropicがフロンティアAIモデルClaude Mythosにより主要OS・ブラウザ等の重要なソフトウェアにおける高深刻度の脆弱性が多数発見されたほか、AIを使用した暗号資産詐欺の大量展開や身元確認・採用プロセスにおけるなりすましの品質向上等の悪用が見られ、AIによる脆弱性探索・悪用の高速化が暗号資産関連業者においても現実的なサイバーリスクとなりつつある
- ゼロデイを含む脆弱性発見が、AIの活用により高速・大量化する一方で、発見された脆弱性に対する事業者側の対応や脆弱性発見者への報酬・評価制度設計の見直しがこれに追いつかない場合、脆弱性発見者との間で協調的な脆弱性開示が成立しにくくなるおそれがある。こうした体制が不十分な場合、脆弱性の報告が放置される、発見者に対する説明や報酬が不十分となる、対応の透明性が確保されないといった問題が生じ得る。その結果、発見者が協調的な開示プロセスから離脱し、脆弱性情報の公開、売却、又は報復的な利用といった非協調的な行動に移行するおそれがある。
- 加えて、攻撃者は、技術的な脆弱性を突いてシステムに侵入するだけでなく、業務運用上の弱点を組み合わせて攻撃を成立させる傾向を強めている。暗号資産業界では、署名鍵管理、出金承認、マルチシグ運用、CI/CD、管理者権限管理等の各プロセスにおいて、人間による判断や承認が重要な役割を果たしている。こうした領域における統制が不十分である場合、攻撃者は、権限の集中、承認フローの迂回、例外処理の悪用、開発・運用環境への不正な変更等を通じて、資産流出や重要情報の窃取につなげることが可能となる。

AIの進展を踏まえ、アタックサーフェスの削減、重要システムの分離、教育・訓練、脆弱性情報開示制度の見直しを含む、技術・運用一体の対策が急務となっている

提言：AI時代の暗号資産サイバーセキュリティ対策

提言

暗号資産関連業者は、外部からの攻撃リスクを最小化するとともに、人間による判断・承認プロセスが攻撃者に悪用されないよう、技術的対策とガバナンス上の統制を一体として整備する必要があるか。具体的には、以下の対応が考えられる。

- **アタックサーフェスの削減：**外部から到達可能なアタックサーフェスを継続的に把握し、不要な公開サービス、設定不備、過剰なアクセス権限を速やかに検知・是正する
- **重要システムのインターネット接続制限：**ウォレット、秘密鍵、署名基盤、認証・権限管理、CI/CD、監視・ログ管理等の利用者資産保全に直結する重要システムについては、外部サービスとの通信を必要最小限に限定し、原則としてインターネットから当該システムへの直接接続は行わない
- **開発環境のセキュリティ管理：**開発環境やCI/CD環境も本番環境への到達経路となり得ることを踏まえ、権限管理、変更承認、ログ監視、サプライチェーンリスク管理を含め、本番環境と同等に重要なセキュリティ管理対象とする
- **重要システムの分離：**本番系、開発・デプロイ系、資産管理系及び管理系の各システムについては、役割やリスク特性に応じて機能を分離し、外部からのサイバー攻撃や一部環境の侵害が発生した場合でも、影響範囲が不用意に拡大しない構成とする
- **証跡の管理：**システム基盤、ネットワーク、セキュリティ設定、権限ポリシー等については、手作業による設定ミスや構成ドリフトを抑制する観点から、可能な範囲でInfrastructure as Code(IaC)を活用し、構成・設定・変更履歴を継続的に把握・検証できる態勢を整備する。その際、IaCコード自体のレビュー、承認、設定不備の検査及び変更管理を実施するとともに、秘密鍵・APIキー等のシークレット情報や個別ユーザーの特権付与については、IaCとは分離した適切な管理を行う必要がある
- **迅速なシステム変更管理：**適切な権限管理、監査可能性及び本番環境の安全性を確保しつつ、緊急時に必要な変更、停止及び復旧を短時間で統制された形で実施できるよう、必要な手続及び技術的な仕組みを整備すべきである（例：ウォレット、署名インフラ、CI/CD、クラウドIAM/KMS、ブリッジ、RPC/DVN設定及びスマートコントラクトのパラメータに関する変更）。
- **トレーニング・教育：**役職員に対する継続的な教育・訓練を実施する。特に、ディープフェイクによるなりすまし、緊急性を装った権限付与依頼、例外的な出金承認依頼、CI/CDや管理者権限に関する不審な変更依頼等について、具体的な確認手順と報告経路を明確化する
- **脆弱性情報開示制度の再設計：**報告品質、検証範囲、開示期限および警察・規制当局との連携を含むResponsible Disclosureの枠組みの再設計を検討する

提言：暗号アジリティ

提言

暗号資産関連業者は、耐量子計算機暗号への移行を見据え、将来的な暗号方式の変更に対応できる体制を整備すべきである。特に、基盤システムの大幅な再設計を伴うことなく暗号アルゴリズムや鍵管理方式を移行できる**暗号アジリティ**を重要なセキュリティ要件として位置付け、中長期的な移行計画を策定することが望ましい

Appendix1. 先行研究

暗号資産関連事業のサイバーセキュリティの特徴を分析する際に、学術界では、システムの階層化モデルを使い、リスクの所在を明らかにするアプローチが多い

先行研究・学術論文 (1/2)

<table>
<tr><th></th><th>学術論文</th><th>著者</th><th>発表関連情報</th><th>定義・分類のアプローチ</th><th>示唆：自律分散型システムの特徴・従来型との違い</th></tr>
<tr><td>1</td><td>A Survey on the Security of Blockchain Systems</td><td>Xiaoqi Li等</td><td>「Future Generation Computer Systems 107」で、2017年8月に発表</td><td>ブロックチェーンシステムにおけるセキュリティ問題を研究する論文であり、下表通り、脅威・攻撃・対策の体系 (Taxonomy) として、層モデルにマッピングして分類している。
<table><tr><th>Risk</th><th>Cause</th></tr><tr><td>51% vulnerability</td><td>Consensus mechanism</td></tr><tr><td>Private key security</td><td>Public-key encryption scheme</td></tr><tr><td>Criminal activity</td><td>Cryptocurrency application</td></tr><tr><td>Double spending</td><td>Transaction verification mechanism</td></tr><tr><td>Transaction privacy leakage</td><td>Transaction design flaw</td></tr><tr><td>Criminal smart contracts</td><td>Smart contract application</td></tr><tr><td>Vulerabilities in small contracts</td><td>Program design flaw</td></tr><tr><td>Under-optimized smart contracts</td><td>Program writing flaw</td></tr><tr><td>Under-priced operations</td><td>EVM design flaw</td></tr></table></td><td>研究で使用する層モデルは、従来の「OS・ネットワーク・アプリ」に加えて、自律分散型システムの技術面特徴である「合意形成・スマートコントラクト」まで拡張した。</td></tr>
<tr><td>2</td><td>SoK: Decentralized Finance (DeFi) Attacks</td><td>Liyi Zhou等</td><td>「2023 IEEE Symposium on Security and Privacy」でカンファレンス発表</td><td>DeFiのセキュリティ攻撃を分析する論文であり、システムモデルにマッピングし、さらに情報アクセス権限により、関係者を「Public／Sequencer／Insider」に分類して、セキュリティ攻撃への防衛能力 (Adversarial capabilities) の1要素として分析している。</td><td>上記#1と同様に、研究で使用する層モデルは、自律分散型システムの技術面特徴である「合意形成・スマートコントラクト」まで拡張した。

さらに、DeFiに関し、従来の「ハッキング」だけでなく、「市場操作 (Market Manipulation)」や「フロントランニング (Front-running)」といった、「コードは正しいが、市場メカニズムや仕様の穴を利用した悪用」もセキュリティの範疇に含めている。（左図におけるPro層とAUX層）

なお、自律分散型システムにおいて情報へのアクセス、および権限管理方法が従来から変遷しているため、その整理も必要だと考えられる。</td></tr>
</table>

暗号資産関連事業のサイバーセキュリティの特徴を分析する際に、学術界では、システムの階層化モデルを使い、リスクの所在を明らかにするアプローチが多い

先行研究・学術論文 (2/2)

	学術論文	著者	発表関連情報	定義・分類のアプローチ	示唆：自律分散型システムの特徴・従来型との違い
3	SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols	Jiahua Xu等	「ACM Computing Surveys/Vol. 55」で2023年発表	自動マーケットメーカー（AMM）形式の分散型取引所のみ研究対象としている論文であるが、類型化したセキュリティ攻撃を、「インフラ層・ミドルウェア層・アプリ層」の3層に簡素化したシステムモデルにマッピングして、リスク要因をグルーピングして分析している。	前葉論文と同様に、階層モデルに自律分散型システムの技術面特徴であるスマートコントラクト等を取り入れている。 さらに、リスク要因の分析において、**ブロックチェーン技術特性の「透明性(Transparency)」と「追跡可能性(Traceability)」から由来するリスクを「Privacy Concern」と定義**し、セキュリティ攻撃の発生要因であると論じている。
4	A Survey on Ethereum Systems Security: Vulnerabilities, Attacks and Defenses	Huashan Chen等	「ACM Computing Surveys/Vol. 53」で2020年発表	Ethereumのセキュリティを研究対象とする論文であり、「システムの層モデル＋環境要因」にマッピングして、セキュリティにおける脆弱性を分析している。 脆弱性のグルーピング・分析において、こまめに発生原因(Causes)を洗い出している。	前述論文と同様に、研究で使用する階層モデルは、自律分散型システム技術特徴の「合意形成」を１つの層として定義し、「スマートコントラクト」等要素も取り入れている。 なお、従来からの「環境要因」を層モデルと別枠でマッピングする観点もある。 従来と比べて、自律分散型システムの新技術に対応して、**「スマートコントラクト・プログラミング」「合意形成メカニズムの設計・運用」等が新しいリスク領域となり、仕様の穴が悪用される可能性**も増えていく。

暗号資産関連事業のサイバーセキュリティの特徴に関し、公的機関・国際機関では、技術的要素だけでなく、ガバナンス、運用と市場、規制等の観点からも分析している

先行研究・公的レポート（1/3）

<table>
<tr><th></th><th>レポート等</th><th>機関名</th><th>発表年月</th><th>定義・分類のアプローチ</th><th>示唆：自律分散型システムの特徴・従来型との違い</th></tr>
<tr><td>1</td><td>NISTIR 8202: Blockchain Technology Overview</td><td>NIST</td><td>2018年10月</td><td>NISTによる、ブロックチェーン技術を体系的に解説する公開文献。

ブロックチェーン技術の特徴を
１）分散方式実装（=中央機関なし、合意形成モデルをもって成り立つ）
２）耐改ざん性が強い（Tamper evident and tamper resistant ）
と要約している。

一方、上記技術的特性が一見「万能」だが、技術問題を超えたところで、
■ 完全な不変性 (Immutability) が保証できない
■ 悪意のあるユーザーへの対処方法
■ コントロールの適用方法
■ 実装の限界
■ データの透明性から生じたコンプライアンス問題
等、運用上およびガバナンス上の制限がある、と論じている。</td><td>ブロックチェーン技術は「合意形成モデルの導入」「分散型権限管理」「データの耐改ざん性と透明性」等特徴を持ち、従来型と決定的に違う。

一方、ブロックチェーン技術の利活用にあたり、運用上およびガバナンス上の制限が多く存在し、場合によってセキュリティを脅かす問題が生じうる。</td></tr>
<tr><td>2</td><td>Crypto Currency Security Standard (CCSS)</td><td>Crypto Currency Certification Consortium (C4)</td><td>Version 9.0
2024年12月</td><td>暗号資産に関する実務標準制定者のC4による最新版「暗号資産を扱う情報システムの標準要件 (CCSS)」は、以下の分類で標準要件を構成している。
<table><tr><th>Category</th><th>Aspect</th></tr><tr><td>1. Cryptographic Asset Management</td><td>1.01 Key Material Generation</td></tr><tr><td></td><td>1.02 Wallet Generation</td></tr><tr><td></td><td>1.03 Key Material Storage</td></tr><tr><td></td><td>1.04 Key Material Access</td></tr><tr><td></td><td>1.05 Key Material Usage</td></tr><tr><td></td><td>1.06 Data Sanitization Documentation</td></tr><tr><td>2. Operations</td><td>2.01 Security Tests/ Audits</td></tr><tr><td></td><td>2.02 Log and Monitor</td></tr><tr><td></td><td>2.03 Governance and Risk</td></tr><tr><td></td><td>2.04 Key Compromise Documentation</td></tr></table></td><td>従来のサーバ防御中心ではなく、自律分散型システムの「取引不可逆（資産が移転されたら取り戻せない）」性質に対応して、「鍵管理・権限管理・ウォレット運用」に関する統制がセキュリティ要件の中核となっている。</td></tr>
</table>

暗号資産関連事業のサイバーセキュリティの特徴に関し、公的機関・国際機関では、技術的要素だけでなく、ガバナンス、運用と市場、規制等の観点からも分析している

先行研究・公的レポート（2/3）

	レポート等	機関名	発表年月	定義・分類のアプローチ	示唆：自律分散型システムの特徴・従来型との違い
3	暗号資産カストディアンのセキュリティ対策についての考え方 － 第5版 －	Cryptoassets Governance Task Force (CGTF)	2024年4月	セキュリティ専門家と暗号資産交換業者の関係者で安全対策基準の策定を目的として設立された研究会CGTFによる、暗号資産カストディアンが利用者の資産を保護する目的としてセキュリティを検討するための推奨事項を整理する公開文献である。 暗号資産カストディ**システムに関する基本的な構成要素や運用フロー等**に沿い、基本モデルを挙げ、分析のベースとしている。 **ブロックチェーン・分散台帳における暗号資産の特徴**について、以下の通り整理している。 ■**署名鍵の重要性**：不可逆な性質を有する暗号資産においては署名鍵の盗難や不正利用、消失に対して、より多くの注意を払う必要がある。 ■**実装の多様性**：暗号資産ごとに仕様が大きく異なり多様であるため、特定の暗号資産には有効な対策手段が、別の暗号資産の仕様では実施できないということも起こりうる。 ■**ブロックチェーンが分岐する可能性**：多種多様な分岐 (fork)、分裂 (split) があり、そのすべてに対応することは困難な場合があり、リスクに応じて対応策を検討する必要がある。 ■**未承認トランザクションに対するリスク**：暗号資産の移転を指示するトランザクションを送信しただけで暗号資産の移転が即座に反映されるわけではなく、トランザクションが承認される必要がある。 **暗号資産の移転において、署名鍵の持つ役割とリスクは極めて大きい**ことから、署名鍵の脅威に関して想定される**脅威の因子とファクターにマッピングして、署名鍵に関するリスクを分析**している。 署名鍵のほか、資産データ・インターネットの基盤・Web PKI・端末環境・ブロックチェーン・外部との業務連携等に係るリスクを分析したうえで、各種リスクに対するセキュリティ管理策について、**ISOにおける情報セキュリティマネジメントシステムの要求事項 ISO/IEC 27001:2013 (JIS Q 27001:2014) および実践のための規範 ISO/IEC 27002:2013 (JIS Q 27002:2014) *を踏襲**して、基本的な考え方を示している。	暗号資産の特徴を踏まえて、**技術的要素と運用と両方の観点から総合的に整理**することで、よりリスクの所在を特定しやすいと考えられる。 暗号資産の特徴は、**「署名鍵の役割」「分散台帳の実装方式」「ブロックチェーン分岐」「合意形成メカニズム」**等にあり、従来型と決定的に違う。 **暗号資産の移転において、署名鍵の持つ役割とリスクは極めて大きい**ため、セキュリティ脅威と対策を分析する際に中核となっている。 自律分散型システムの特徴・従来型との違いを踏まえ、**既存のセキュリティ基準へマッピング**する等分析手法は、リスク特定と対策検討に大いに役立つと思われる。

*参照時点の規格版であり、現行版はISO/IEC 27001:2022＋Amd 1:2024（JIS Q 27001:2025）およびISO/IEC 27002:2022（JIS Q 27002:2024）である。

暗号資産関連事業のサイバーセキュリティの特徴に関し、公的機関・国際機関では、技術的要素だけでなく、ガバナンス、運用と市場、規制等の観点からも分析している

先行研究・公的レポート（3/3）

<table>
<tr><th></th><th>レポート等</th><th>機関名</th><th>発表年月</th><th>定義・分類のアプローチ</th><th>示唆：自律分散型システムの特徴・従来型との違い</th></tr>
<tr><td>4</td><td>The crypto ecosystem key elements and risks</td><td>BIS</td><td>2023年7月</td><td>暗号資産の安全性に関し、
■ 暗号資産エコシステムに閉じるリスク
■ DeFiにおけるリスク
■ 伝統的金融機関との連携におけるリスク
■ 新興市場等と関連するリスク
に要素分解して分析している。</td><td>技術問題に閉じず、エコシステム構造・仲介者・市場ダイナミクスがリスクを増幅しうると整理している。</td></tr>
<tr><td>5</td><td>Quarterly Review - DeFi risks and the decentralisation illusion</td><td>BIS</td><td>2021年12月</td><td>DeFiにおけるリスクを、下表にて機能別・サービス別にプレーヤーをマッピングして、従来の伝統的金融業務と比較しながら分析し、中央集権的な要素があることから、「分散化の幻想 (Decentralisation illusion) 」を指摘した。
Crypto vs traditional financial system
<table><tr><th rowspan="2">Function</th><th rowspan="2">Service</th><th colspan="2">Crypto financial system</th><th rowspan="2">Traditional finance</th></tr><tr><th>Decentralised finance (DeFi)</th><th>Centralised finance (CeFi)</th></tr><tr><td rowspan="3">Trading</td><td>Funds transfer</td><td>DeFi stablecoins (DAI)</td><td>CeFi stablecoins (USDT, USDC)</td><td>Traditional payment platforms</td></tr><tr><td>Asset trading</td><td>Crypto asset DEX (Uniswap)</td><td rowspan="2">Crypto CEX (Binance, Coinbase)</td><td rowspan="2">Exchanges and OTC brokers</td></tr><tr><td>Derivatives trading</td><td>Crypto derivatives DEX (Synthetix, dYdX)</td></tr><tr><td rowspan="2">Lending</td><td>Secured lending</td><td>Crypto decentralised lending platforms (Aave, Compound)</td><td>Crypto centralised lending platforms (BlockFi, Celsius)</td><td>Broker-dealers active in repo and securities lending</td></tr><tr><td>Unsecured lending</td><td>Crypto credit delegation (Aave)</td><td>Crypto banks (Silvergate)</td><td>Commercial banks and non-bank lenders</td></tr><tr><td>Investing</td><td>Investment vehicles</td><td>Crypto decentralised portfolios (yearn, Convex)</td><td>Crypto funds (Grayscale, Galaxy)</td><td>Investment funds</td></tr></table>CEX = centralised exchanges; DEX = decentralised exchanges; OTC = over-the-counter; USDC = USD Coin; USDT = Tether.</td><td>自律分散型システム技術は分散方式で実装されるが、金融サービスを提供するために登場する各プレーヤー（ウォレット事業者、CEX、連携する伝統的金融機関等を含む）において、リスク管理と規制対応の観点から、中央集権的なガバナンスを構築している。

なお、自律分散型システム技術の特徴である「合意形成メカニズム」自体も、決定権限を持つものに集中する傾向がある (favours a concentration of decision power)。</td></tr>
</table>

Appendix2. 機能別リスク評価

暗号資産関連事業特有の構造的脆弱性を可視化するために、多面的なリスクファクターを織り込み、サイバーリスクの集中点を評価した

暗号資産関連機能に対するサイバーリスク評価

目的

- 暗号資産関連のエコシステムにおいて「どこが構造的に狙われやすいか」を1.3で整理した暗号資産関連サービスの機能ごとに可視化することを目的とする
- 従来の「影響度 × 発生可能性」の単一スコア化ではなく、機能ごとのリスク特性の違い（質的差異）を明確にすることを重視する

前提

- エコシステム全体のリスク集中点を把握するための分析枠組みであり、**特定サービスの安全性ランキングではなく、各サービスの利用可否を示すものでもない**
- 本評価は事業者の典型的なサービスを前提にしており、**多様な事業形態を持つ個別事業者の安全性を包括的に保証するものではない**
- 規制の有無や運営体制により、同一カテゴリの事業者でも実際のリスクは異なる
- 技術の進化や新たな脅威の発生により、相対的なリスク水準は将来変動し得る

評価アプローチ

リスクファクターは以下の観点で選定した

(1)攻撃者視点	攻撃の動機（資産集中） 攻撃の容易性（攻撃面）
(2)システム構造視点	障害の波及範囲（波及性） 権限の集中・統治構造
(3)防御体制視点	外部監査の有無（規制等の適用外） 人的・運用的脆弱性（人的・運用要因）

また、以下の公的・国際的枠組みを参照して構成

- NIST SP 800-30（リスク評価）
- NIST SP 800-53（セキュリティ統制カタログ）
- NIST CSF 2.0（６つの機能モデル等）
- BIS／FSB（DeFiの相互接続性リスク）
- ENISA／Verizon DBIR（人的要因）

既存の国際基準をベースとしつつ、分散型システムの特性（不可逆性、コンポーザビリティ等）を加味して独自に選定

選定したリスクファクター

①資産集中	攻撃者にとって“どれだけ魅力的な標的か”
②波及性	破られた場合、どこまで連鎖するか
③攻撃面	外部から侵入可能な接点はどれだけ広いか
④規制等の適用外	独立した監査・規制・第三者検証は機能しているか
⑤人的・運用要因	技術以外の要素で破綻しうるか

※各ファクターを「高・中・低」で評価し、単一スコア化は行わない
※最弱点原理（システム全体の安全性は構成要素の中での最弱点によって決定）を前提とする

想定される活用方法

- 規制・監査：重点確認領域・検証観点の整理
- 事業者　　：自社リスクの俯瞰と対策優先度付け
- 委託管理　：重要依存先の確認観点補助

暗号資産関連事業特有の構造的脆弱性を可視化するために、選定したリスクファクターごとに、それぞれのサイバーリスクを高・中・低の３段階で定性的に評価した

リスクファクターの定義とレベル

①資産集中

システム内における特定資産の重要性、および資金・データ集中により攻撃の主要標的となる度合い

レベル	内容
高	莫大な顧客資産や重要データが単一拠点やコントラクトに集中する状態
中	一定の資産を保持するが分散化され、単一障害時の被害が限定的な状態
低	顧客資産を直接保持せず、侵害時の直接的な経済的損失が微小な状態

②波及性

外部システムや他プロトコルとの依存関係の強さと、一部の障害や侵害が全体へ連鎖的に被害を広げるリスクの規模

レベル	内容
高	エコシステムの基盤として機能し、障害が他システムへ壊滅的影響を及ぶ
中	複数システムと接続しているが、影響は特定サービスやユーザーに留まる
低	独立して稼働する要素が強く、他システムへの波及効果が極めて小さい

③攻撃面

攻撃者がシステムへ侵入したり、不正操作を行ったりするために、外部からアクセス可能な接点（エンドポイント等）の多さと露出の広さ

レベル	内容
高	コントラクトやAPI等外部からアクセス可能な通信接点が非常に多い
中	外部接点は存在するが機能が単一であり、アクセス制御により攻撃を抑制
低	外部ネットワークとの接点が極小、または物理的に隔離され攻撃が困難

④規制等の適用外

規制当局の監督や第三者による独立監査の対象となり、外部から継続的に検証・統制されている度合い

レベル	内容
高	規制監督や第三者監査の対象外であり、外部からの統制がほとんど存在しない状態
中	一定の規制対応や第三者レビューはあるが、継続的な監督体制は限定的な状態
低	法令に基づく規制監督下にあり、定期的な第三者監査が実施されている状態

⑤人的・運用要因

フィッシング等の心理的な隙、運用手順の不備、設定ミス等に起因する人為的リスク

レベル	内容
高	ユーザーのITリテラシーに依存し、操作ミスやフィッシング被害が甚大
中	専門家が運用するが、複雑な設定ミスやソーシャルエンジニアリング的な攻撃の標的となる
低	運用プロセスが自動化・厳格化され、人的介入の余地が少なくエラーが起こりにくい

※ 本評価は定量的指標によらず定性的観点から整理したものであり、評価結果には一定の主観的要素が含まれる可能性がある点に留意が必要

ユーザーアクセス層は、人的・運用的要因が主要な突破口となりやすく、運用体制の厳格性が流出リスクの高低に大きく影響する

機能別リスク評価（1/4）：ユーザーアクセス層

機能	代表プレイヤー	主な役割	なぜ狙われるか・脆弱性の所在	リスクプロファイル	①資産集中	②波及性	③攻撃面	④規制の適用外	⑤人的・運用	MITRE AADAPTの代表例
CEX	Binance Coinbase BitGo	売買・カストディ・法定通貨交換	ユーザー資産と個人情報(KYC)が集中する巨大な資産集中点。外部攻撃に加え、内部犯行やAPIキー流出等攻撃ベクトルが多岐にわたる	**顧客資産の集中と比較的広い攻撃面により標的化されやすく、人的・運用的要因が損害に結び付く可能性**がある。一方、外部の監査が機能する場合には是正や抑止が働く余地も見込まれ、資産集中・攻撃面・人的要因の組み合わせが主要なリスク構造となり得る	高	中	高	低	高	■ Acquire Accounts (ADT3001)：偽造IDや盗難IDによるアカウント取得 ■ Scrape KYC Data (ADT3026)：個人情報の収集・流出 ■ Intercept API Communication (ADT3018)：APIキーや通信の傍受 ■ Insider-Assisted Access (ADT3017)：内部者を悪用したアクセス ■ Aggregate Private Key Generation Data (ADT3002)：鍵生成プロセスの解析・エントロピー不足の悪用
SW ウォレット	Metamask Phantom Safe	鍵管理・署名インターフェース	常にネット接続されており、フィッシング・マルウェア・承認(Approve)の誤認を狙いやすい。個人資産全損の最頻出ポイント	資産自体は保持しないものの**署名権限が集中**しやすく、攻撃面や波及性に加えて**人的・運用的要因の影響を受けやすい**。外部の監査等は限定的な場合が多く、利用者の誤操作や詐欺誘導が損失につながる可能性がある	中	中	高	中	高	■ Manipulate Transaction History: Address Poisoning (ADT3020.001)：類似アドレスによる誤送金誘導 ■ Manipulate Transaction History: Zero-Value Transfer Phishing (ADT3020.002)：承認や送金を誤認させるフィッシング ■ Unsecured Credentials: Private Keys (ADT1552.004)：マルウェア等による署名鍵の窃取
DEX／DeFi UI	Uniswap UI GMX UI Jupiter	取引操作のフロントエンド	サプライチェーン攻撃、DNSハイジャックにより、ユーザーに悪意ある署名を誘導する。資産そのものは保持しないが、最大の侵入経路	資産集中は小さい一方、**複数プロトコルへの接続により波及性が生じやすく**、人的・運用的要因を通じて**不正誘導が発生する可能性**がある。**外部の規制が弱い**事例も多く、フロントエンドという入口部分の攻撃面管理が重要	低	中	中	高	高	■ Supply Chain Compromise (ADT1195)：UIライブラリへの悪意あるコード注入 ■ Exploit External Services (ADT3008)：フロントエンド（ウェブサイト）の脆弱性悪用やフィッシング ■ Supply Chain Compromise: Compromise Software Dependencies and Development Tools (ADT1195.001)：依存関係の汚染
HW ウォレット	Ledger Trezor Keystone	物理デバイス内での保管・署名	オフライン前提のため遠隔侵害は極めて困難。ただし、物理的なサプライチェーン攻撃や、リカバリーフレーズの保管ミス(アナログ流出)はリスク	攻撃面と波及性は比較的抑制される傾向がある一方、**紛失や管理不備といった人的・運用的要因**が主なリスクとなり得る。外部の監査は製品レベルに限定される場合が多く、利用者側の運用品質が安全性に影響する可能性がある	中	中	中	中	中	■ Supply Chain Compromise (ADT1195)：物流過程でのデバイス改ざん ■ Fault-Injection Attack (ADT3014)：電圧操作等によるグリッチ攻撃 ■ Side-Channel Attack (ADT3027)：サイドチャネル攻撃 ■ Exploit Obsolete Device (ADT3010)：更新されていないFWの脆弱性悪用

機能別リスク評価（1/4）：ユーザーアクセス層

機能区分	資産集中	波及性	攻撃面	規制の適用外	人的・運用
CEX／カストディ	高	中	高	低	高
	顧客資産や重要情報が特定の運用基盤に集約される場合、主要な攻撃対象となり得る。	複数の外部システム（決済・入出金・市場接続等）と連携することが多く、影響が特定の範囲に波及する可能性がある。	公開APIやユーザー向け機能が多く、外部から到達可能な接点が相対的に増えやすい。	金融規制下で運営され、外部監査や当局報告が求められる場合が多く、一定の外部の規制が機能する可能性がある。	内部不正、運用ミス、フィッシング等の人的要因が損害に直結しやすい局面がある。
SWウォレット	中	中	高	中	高
	資産自体はチェーン上にあるが、署名権限が端末やアプリに集中する場合、攻撃対象として注目され得る。	多様なアプリケーションとの連携点となり、影響が利用者や特定サービスに及ぶ可能性がある。	ブラウザ拡張・モバイルアプリ等として外部環境と接するため、露出する接点が広がりやすい。	一部の提供主体では監査やガバナンス体制が整備される場合もあるが、OSS主体の実装では継続的な外部の規制が限定的となる可能性がある。	利用者の判断・操作に依存する局面が大きく、詐欺誘導や誤操作が被害に結びつきやすい。
DEX／DeFi UI	低	中	中	高	高
	UI自体が顧客資産を直接保持しない場合、資産集中による直接損失は相対的に限定的と考えられる。	複数プロトコルへの接続経路となることが多く、影響が特定の利用者群に波及する可能性がある。	外部公開されたフロントエンドであり改ざん等の対象となり得るが、機能は比較的限定される場合がある。	プロトコル主体で運営される場合が多く、規制監督や定期的な第三者監査が存在しない事例が一般的である。	利用者が承認内容を正確に判別しづらい局面があり、不正誘導が被害につながる可能性がある。
HWウォレット	中	中	中	中	中
	資産はチェーン上にあるが、署名権限の保管手段として狙われ得る（特に供給網・偽装等の観点）。	基本オフライン運用が前提であればリスクは低いが、オンライン署名の場合はトランザクション情報の真正性が確保できなければ影響が波及する可能性がある。	リモート到達性は限定されるも、攻撃には物理的接近や利用者介在があり得る。	製品レベルでの監査や評価は実施される場合があるものの、利用段階における継続的な外部監督は限定的となる可能性がある。	紛失・盗難・不適切保管等のアナログ要因が残り、一定の人的リスクが見込まれる。

DeFi-プロトコルに高い資産集中度が見られ、さらに監査・監督の対象外とされていることから、エコシステム全体の中で大きなリスク要因となっている

機能別リスク評価（2/4）：アプリケーション＆コントラクト層

機能	代表プレイヤー	主な役割	なぜ狙われるか・脆弱性の所在	リスクプロファイル	①資産集中	②波及性	③攻撃面	④規制の適用外	⑤人的・運用	MITRE AADAPTの代表例
DeFiプロトコル	Uniswap Aave Lido EigenLayer	金融ロジック・ステーキング運用	スマートコントラクトに巨額のTVLが集中。ロジックバグ、リエントランシー攻撃。特に、LST／リステーキングなどは資産ロックと運用ロジックに起因する二重のリスクを抱える	**資産集中・波及性・攻撃面が同時に高まりやすく、外部の規制も限定的**である場合、インシデント時の影響が広範に及ぶ可能性がある。設計・実装・運用の成熟度が残余リスクに大きく影響し得る領域と考えられる	高	高	高	高	中	■ Exploit Smart Contract Implementation: Reentrancy (ADT3012.005)：再入攻撃による資金引き出し ■ Exploit Smart Contract Implementation (ADT3012)：実装バグの悪用 ■ Flash Loan (ADT3015)：フラッシュローンを利用した価格操作や攻撃 ■ Smart Contract Implementation Analysis (ADT3029)：コード解析による脆弱性発見
トークン発行体	Circle Tether Ondo	資産裏付け・発行・凍結管理	コントラクト自体は堅牢だが、管理用署名鍵が流出すると不正発行や不正凍結が可能。サイバー攻撃のほか内部統制・ガバナンスリスクも抱える	**裏付け資産や発行残高の集中**と比較的高い波及性により、**単一主体への依存**が生じる可能性がある。一方、外部の規制が機能する場合には被害軽減や是正の余地も見込まれ、内部運用の品質が実務上のリスク水準に影響し得る	高	高	中	低	中	■ Unsecured Credentials: Private Keys (ADT1552.004)：管理用署名鍵の流出 ■ Generate Counterfeit Tokens (ADT3016)：不正なトークン発行 ■ Exploit Smart Contract Implementation: Contract Ownership Changes (ADT3012.001)：権限乗っ取りによる不正操作
DAO運営	Uniswap DAO MakerDAO	パラメータ変更・資金配分	ガバナンストークンの買収やフラッシュローンによる「提案乗っ取り」。プロトコルのアップデート権限を悪用し、正当な手続きで資金を抜く	形式上は分散されていても、**人的・運用的要因や情報非対称により意思決定が歪む可能性**がある。外部の規制は限定的であり、波及性と参加者行動がリスクの中核となり得る	中	中	中	高	高	■ Flash Loan (ADT3015)：大量資金を借入れて提案を可決させるガバナンス攻撃 ■ Exploit Smart Contract Hierarchical Ownership (ADT3011)：階層的な所有権構造の悪用 ■ Exploit Smart Contract Implementation: Contract Ownership Changes (ADT3012.001)：パラメータ変更権限の奪取

機能別リスク評価（2/4）：アプリケーション＆コントラクト層

機能区分	資産集中	波及性	攻撃面	規制の適用外	人的・運用
DeFi & LSTプロトコル	高	高	高	高	中
	TVL等の価値がコントラクトに集約される場合、攻撃の主要標的となり得る。	他プロトコルとの連鎖利用が前提となることが多く、一部障害が広範に波及する可能性がある。	公開ロジック・複雑な状態遷移を持つため、外部からの悪用余地が相対的に大きい。	自律的に運用される構成が多く、規制監督や継続的な第三者監査が存在しない場合が一般的である。	設計・実装・デプロイの不備が重大影響になり得るが、体制成熟度により差が出やすい。
トークン発行体	高	高	中	低	中
	裏付け資産や発行残高が大きい場合、単一主体に価値・信用が集約し得る。	基軸資産として利用される場合、市場や多くのサービスに広く影響する可能性がある。	スマートコントラクト等の外部接点はあるが、機能は比較的限定される場合がある。	法人主体として規制監督や会計監査を受ける場合が多く、一定の外部の監査が働く可能性がある。	内部統制・手続に依存するため、運用不備や内部者リスクが残る可能性がある。
DAO運営	中	中	中	高	高
	トレジャリーを保有する場合があるが、規模や流動性により集中度は変動し得る。	パラメータ変更等が対象システムへ影響し得るが、影響範囲は設計に依存する。	投票・フォーラム等の接点があり、攻撃・攪乱の対象となり得る。	法的主体が不明確な場合が多く、規制監督や第三者による継続的統制が限定的となる可能性がある。	無関心・情報非対称・ソーシャルエンジニアリング等により意思決定が歪む可能性がある。

クロスチェーン（ブリッジ）は、異なるチェーン間の資産を橋渡しする構造上、資産集中・波及性が高く、単一点の破綻が広範な連鎖的被害に直結しやすい

機能別リスク評価（3/4）：ミドルウェア＆インフラサービス層

機能	代表プレイヤー	主な役割	なぜ狙われるか・脆弱性の所在	リスクプロファイル	①資産集中	②波及性	③攻撃面	④規制の適用外	⑤人的・運用	MITRE AADAPTの代表例
クロスチェーン（ブリッジ）	LayerZero Wormhole Across	チェーン間資産転送・中継	ブリッジコントラクトに巨額資産がロックされ、かつ検証ロジックが極めて複雑。過去の被害額トップ事例が集中しており、最も実入りが良い	**ロック資産の集中、高い波及性、広い攻撃面**が同時に成立しやすく、外部の規制も弱い場合には影響が広範に及ぶ可能性がある。実装品質と運用体制がリスク水準に大きく影響し得る	高	高	高	高	中	■ Exploit Smart Contract Implementation: Signature Replay Attack (ADT3012.006)：署名の再利用による不正出金 ■ Exploit Blockchain Technology Specific Vulnerabilities (ADT3013)：チェーン固有の仕様（検証ロジック）の悪用 ■ Cross-Chain Swaps (Hopping) (ADT3005)：攻撃者の資金移動手段だが、ブリッジの脆弱性をつく文脈も含む
鍵管理サービス	Fireblocks Copper Dfns	鍵分散管理・署名基盤提供	CEXや機関の署名鍵シェアを管理する中枢。実装バグ、設定ミス、内部不正があれば、顧客資産を一括で抜き取れる技術的な単一障害点となり得る	資産は直接保持しなくても、**署名権限が集中する**場合には。鍵管理の重要性が高まり、基盤としての波及性も大きくなる可能性がある。外部の規制が一定程度機能する場合もあるが、複雑な運用フローに起因する**人的要因が残る**ことがある	中	高	中	中	中	■ Exploit External Services (ADT3008)：外部サービスの脆弱性の悪用 ■ Aggregate Private Key Generation Data (ADT3002)：鍵生成プロセスの解析・エントロピー不足の悪用 ■ Insider-Assisted Access (ADT3017)：内部者を悪用したアクセス ■ Unsecured Credentials: Private Keys (ADT1552.004)：分散管理された鍵の復元・流出
オラクル	Chainlink Pyth RedStone	オフチェーン価格情報の供給	価格フィードの操作・遅延により、DeFi側で誤った清算や裁定取引を誘発させる。資産を直接持たないが、市場破壊のトリガーとなる	資産集中は小さいものの、**価格参照元としての波及性**が高くなる場合がある。外部の規制は限定的な事例も多く、データ品質や運用設定の不備が広範な影響を生む可能性がある	低	高	中	高	中	■ Exploit Smart Contract Implementation: Oracle Manipulation (ADT3012.004)：外部データソースの改ざんによる価格操作 ■ Smart Contract Implementation Analysis: Oracle Analysis (ADT3029.005)：依存するオラクルの特定と脆弱性調査
ZK／スケーリング	zkSync Polygon Zero	証明生成・検証・圧縮	暗号学的証明の回路(Circuit)にバグがあった場合、偽の証明で不正出金が可能。技術的難易度は極めて高い	**基盤性が高く波及性が大きくなる**一方、外部の規制は弱い場合がある。攻撃面は実装構成に依存し、集中し得る運用要素や人的・運用的要因がリスク水準を左右する可能性がある	低	高	中	高	低	■ Exploit Blockchain Technology Specific Vulnerabilities (ADT3013)：新しい技術（回路等）固有のバグ悪用 ■ Generate Counterfeit Tokens: Cryptographic Protocol Analysis (ADT3016.001)：暗号プロトコルの解析による偽装（ZK証明の偽造等）
RPC／ノードAPI	Infura Alchemy QuickNode	APIアクセス・Tx中継	資産へのアクセス権はない。主にサービス拒否（DoS）や、フィッシングサイトと連携した情報の偽装に使われる	資産集中は小さいものの、**通信要衝**として波及性と攻撃面が大きくなり得る。代替経路が存在する場合もあるが、特定事業者への依存度と運用品質が実務上のリスク感に影響しやすい	低	高	高	中	低	■ Eclipse Attack (ADT3006)：ノードへの情報を遮断・偽装し、誤った情報を与える ■ Exploit Gas-Free RPCs (ADT3009)：特権RPCへの不正アクセス ■ Intercept API Communication (ADT3018)：通信経路上でのデータ傍受

機能別リスク評価（3/4）：ミドルウェア＆インフラサービス層

機能区分	資産集中	波及性	攻撃面	規制の適用外	人的・運用
クロスチェーン（ブリッジ）	高	高	高	高	中
	ロック資産が集約される構造となりやすく、主要標的になり得る。	複数ネットワークを直結するため、一方の問題が他方へ波及し得る。	検証ロジックや接点が複雑化しやすく、外部からの攻撃余地が増え得る。	規制枠組み外で運営される例が多く、外部からの継続的な検証や統制が十分に及ばない可能性がある。	実装・運用が高度であるため、設計不備や運用ミスが影響し得る。
MPC／鍵管理インフラ	中	高	中	中	中
	資産を直接保持しない場合でも、署名権限が集約されることで重要性が高まり得る。	複数事業者の基盤として利用される場合、障害・侵害の影響が広がる可能性がある。	アクセス制御により抑制される一方、管理面の接点が残り得る。	法人向けサービスではSOC等の監査対象となる場合もあるが、運用実態に対する継続的な監査の範囲は事業者により差が生じ得る。	承認フローや運用手順が複雑化しやすく、人的ミスや手続不備が影響し得る。
オラクル	低	高	中	高	中
	通常は資産を保持せず、資産集中による直接損失は限定的と考えられる。	価格参照元として多数のプロトコルが依存する場合、影響が広範に波及し得る。	データ取得元・ノード運用等の接点があり、一定の露出が生じ得る。	一部では監査が実施される場合もあるが、継続的な監督体制は限定的となる事例が多い。	自動化される場合でも、運用・設定・対応判断が残り得る。
ZK／スケーリング	低	高	中	高	低
	ブリッジ等の周辺で資産が集約される場合があり、集中度は構成に依存し得る。	L1／L2間の基盤として多くの利用が集まる場合、影響が広範に波及し得る。	暗号学的実装・運用接点があり、一定の攻撃余地が残り得る。	プロトコル主体で運営される構成が多く、規制監督や定期監査が存在しない場合が一般的である。	自動化が進む場合、人的介入は相対的に少ないが、実装ミス等は別途考慮が必要。
RPC／ノードAPI	低	高	高	中	低
	通常は資産を保持せず、資産集中による直接損失は限定的と見込まれる。	ユーザーとネットワークを結ぶ通信要衝となり、障害が広範に影響し得る。	公開アクセスが多く、DDoS等の対象となりやすい。	大手事業者ではSOC等の監査体制が整備される場合もあるが、全体としては事業者依存の統制水準となり得る。	標準的運用で自動化されることも多いが、設定・運用判断の影響は残り得る。

ブロックチェーン層における波及性は高いものの、TX順序制御等を除けば、攻撃の成立が難しい場合が多い。一方、ソフトウェア供給源は攻撃面が広く、悪意あるコードが混入すると、多数のプロジェクトへ被害が波及しやすい

機能別リスク評価（4/4）：ブロックチェーン層、横断的基盤・環境

機能	代表プレイヤー	主な役割	なぜ狙われるか・脆弱性の所在	リスクプロファイル	①資産集中	②波及性	③攻撃面	④規制の適用外	⑤人的・運用	MITRE AADAPTの代表例
Tx順序制御(MEV／Seq)	Flashbots L2 Sequencer	トランザクション順序制御	シーケンサー（中央集権的サーバ）の検閲・停止リスク。MEV（サンドイッチ攻撃）によるユーザー利益の搾取	資産保管は行わないものの、市場全体への波及性が高くなる可能性がある。外部の規制は限定的で、**設計の透明性や運用方針がリスク水準に影響**し得る	中	高	中	高	中	■ Market Manipulation (ADT3021)：サンドイッチ攻撃等の市場操作 ■ Smart Contract Implementation Analysis: Timestamp Dependence Analysis (ADT3029.006)：順序やタイムスタンプ依存の悪用 ■ Induce Legal and Regulatory Penalties (ADT3019)：検閲による規制違反リスクの誘発
コンセンサス(Validator)	Coinbase Cloud Figment	ブロック生成・検証	バリデータ鍵の流出によるスラッシング(資産没収)。ステーク集中時は検閲や再編成(Reorg)のリスクが高まる	合意形成基盤として波及性が大きく、ステーキング資産の集中度は参加構造により変動し得る。外部の規制は運営形態により差があり、**鍵管理やインフラ運用といった人的・運用的要因が事故要因**となる可能性がある	中	高	中	高	中	■ Exploit Consensus Logic (ADT3007)：コンセンサスの脆弱性悪用 ■ Chain Reorganization (ADT3003)：チェーンの再編成によるトランザクションの無効化 ■ Unsecured Credentials: Private Keys (ADT1552.004)：バリデータ鍵流出によるスラッシング
L1／L2ネットワーク	Ethereum Solana Optimism	台帳記録・コンセンサス	主要チェーンへの51%攻撃は国家予算レベルのコストが必要で非現実的。ただし、マイナーなチェーンでは安価に実行可能	**資産集中・波及性・攻撃面が高くなりやすい基盤層**であり、外部の規制は限定的な場合が多い。分散性が一定の緩和効果を持つこともあるが、プロトコル品質と運用実態が残余リスクに影響し得る	高	高	中	高	低	■ Exploit Consensus Logic: Circumvent Voting Majority Control (ADT3007.001)：51%攻撃 ■ Exploit Consensus Logic: Double-Spending Attack (ADT3007.002)：二重支払い攻撃 ■ Exploit Consensus Logic: Sybil Node Creation (ADT3007.004)：大量の偽ノードによるネットワーク支配
物理基盤インフラ(クラウド／HSM)	AWS Thales CloudHSM	サーバー・NW・物理鍵保護	攻撃目的は資産盗難ではなく「稼働停止(DoS)」や物理的破壊。HSMは突破されれば致命的だが、事例は極めて稀	上位層の依存が集中しやすく波及性が高くなる一方、外部の監査や運用成熟度は比較的高い場合が多い。**特定事業者への集中や管理API等の攻撃**面が主な論点となり得る	中	高	中	低	低	■ Fault-Injection Attack (ADT3014)：物理的ストレスによる誤作動誘発 ■ Side-Channel Attack (ADT3027)：物理的情報漏洩 ■ Reputation Damage (ADT3024)：稼働停止（DoS）による信用毀損
ソフトウェア供給源	OSS npm GitHub	ソフトウェアの開発・コード管理・ライブラリ	依存関係を悪用したサプライチェーン攻撃。悪意あるコードが混入された場合。それを利用する多数のプロジェクトに被害が波及	外部の規制が限定的な中で、公開環境としての攻撃面の広さや人的・運用的要因が**サプライチェーン攻撃の標的とされやすく、広範なシステムへの連鎖的な被害を引き起こす要因**となり得る	低	高	高	高	高	■ Supply Chain Compromise (ADT1195)：オープンソースの依存関係やソースコードリポジトリに対する悪意あるコードの混入 ■ Exploit External Services (ADT3008)：サードパーティプロバイダー等の外部サービスの脆弱性を悪用した、広範な接続システムへの初期アクセス権の取得

機能別リスク評価（4/4）：ブロックチェーン層、横断的基盤・環境

機能区分	資産集中	波及性	攻撃面	規制の適用外	人的・運用
Tx順序制御 (MEV／Seq)	中	高	中	高	中
	資産保管ではないが、価値抽出機会が集中し得るため、標的化の要因となり得る。	取引順序が市場挙動に影響し得るため、広範な波及が生じ得る。	通信・運用接点があり、一定の攻撃余地が残り得る。	明確な統制・監督の枠組みが存在しない構成が多く、外部からの継続的な検証は限定的となる可能性がある。	自動化が進む場合がある一方、設計・透明性の問題は別途残り得る。
コンセンサス (Validator)	中	高	中	高	中
	ステーキング資産が集約される場合があり、集中度は分布により変動し得る。	合意形成の基盤として機能し、障害がネットワーク全体へ影響し得る。	P2P通信や運用基盤があり、一定の攻撃余地が残り得る。	法人運営の場合は一定の統制が働く可能性がある一方、個人運営ノードでは外部の規制が及ばない事例も見られる。	鍵管理・運用設定の不備が事故要因となり得る。
L1／L2 ネットワーク	高	高	中	高	低
	全体の価値・活動が基盤層に集約されやすく、重大インシデント時の影響が大きくなり得る。	全アプリケーションの実行基盤であり、障害が広範に波及し得る。	コンセンサスから実行まで層が広く、攻撃対象領域が増え得るが、攻撃が困難な場合が多い。	分散型プロトコルとして運営される場合が多く、規制監督や継続的な第三者統制が存在しない可能性がある。	プロトコル自動実行が中心となるが、運用・実装起因の要素は別途残り得る。
物理基盤インフラ (クラウド／HSM)	中	高	中	低	低
	ノードや鍵が特定基盤に集約される場合があり、集中度は採用状況に依存し得る。	上位層が広く依存するため、障害が波及し得る。	厳格な制御が前提でも、管理API等の外部接点が残り得る。	第三者認証や監査制度が整備されている場合が多く、比較的高い外部監査水準が期待され得る。	高度な運用手順が整備される傾向にあるが、ゼロではなく運用品質に依存し得る。
ソフトウェア 供給源	低	高	高	高	高
	直接的な顧客資産は保持しないため、資産集中による直接的な経済的損失は限定的と考えられる。	多数のプロジェクトが依存する基盤として機能することが多く、障害や侵害がエコシステム全体へ広範に波及する可能性がある。	公開リポジトリやパッケージマネージャーとして広くアクセス可能であり、不正コード混入等の外部接点が相対的に多くなり得る。	オープンソースやコミュニティ主導で運営される場合が多く、規制監督が限定的となる傾向がある。	開発者のアカウント管理不備やソーシャルエンジニアリング等、人為的な隙がサプライチェーン攻撃に結びつきやすい局面がある。

Appendix3. MITREフレームワーク

MITREフレームワークは、攻撃・検知・防御を統合的に整理し、セキュリティ対策の網羅性と有効性を評価するための基盤となる

MITRE ATT&CK®、MITRE AADAPT™、MITRE D3FEND ™の概要

MITRE とは

米国の非営利団体であり、米国連邦政府等の公共機関に対してサイバーセキュリティ、国家安全保障、医療等の分野における研究開発等の支援を行っている。
サイバーセキュリティ分野の支援では、攻撃者の技法を体系化したフレームワークや、CVEといった脆弱性管理プログラム等がある

攻撃	MITRE ATT&CK® (*1)	■ システムに対する攻撃者の戦術（Tactics）と技法（Techniques）を、実世界の観測に基づき体系化した包括的なフレームワーク ■ 攻撃手法を偵察・リソース開発・初期アクセス等の戦術種別で分類し、各技法にサブテクニック、緩和策（Mitigations）、検知策（Detections）を紐づける ■ Enterprise／Mobile／ICS（産業用制御システム）といったシステムの領域ごとに戦術・技法を体系化している
	MITRE AADAPT™ (*2)	■ 暗号資産等のデジタル資産管理システムにおける攻撃者の戦術（Tactics）と技法（Techniques）を体系化した包括的なフレームワーク ■ MITRE ATT&CK®のモデルをベースに、デジタル資産特有の攻撃観点を補完する ■ 11の戦術とそれに基づく技法から構成され、緩和策、検知策の説明や、Enterprise／Mobile／ICSといったシステムの領域ごとの戦術・技法の記載はない
防御	MITRE D3FEND™ (*3)	■ MITRE D3FENDは、防御の技術・手法（Countermeasures）を体系化したナレッジベース ■ ATT&CKの攻撃技法に対し、検知・防止・対応の具体策を紐付けて整理できるフレームワーク

本研究調査での活用

- 暗号資産関連事業に関するサイバー攻撃事例分析において、該当する攻撃手法を整理する
- 暗号資産関連業者にとって実効性のある対応策、改善案を導くための参考とする
- 本研究調査ではEnterpriseの領域のみ（MITRE ATT&CK®）を対象としている

(*1): MITRE ATT&CK® : MITRE Adversarial Tactics, Techniques, and Common Knowledge
(*2): MITRE | AADAPT™: MITRE Adversarial Actions in Digital Asset Payment Technologies
(*3): MITRE D3FEND™: MITRE Digital Defensive Framework for Enterprise Network

MITRE ATT&CK®は、システムに対する攻撃者の「戦術」と「技法」を実観測に基づき体系化した知識ベースである

MITRE ATT&CK®の戦術と技法（1/2）

戦術と技法
Tactics & Techniques

- 戦術とは、侵害や攻撃の各局面における、敵対者の戦術的な目標（意図）を指す概念である。技法の「なぜ（Why）」、すなわち攻撃者がその行動を取る理由を表す。全14カテゴリに整理されており、攻撃の目的面で段階・狙いを区分する枠組みであり、各戦術ごとに達成のための具体的手段（技法）が紐づく
- 技法とは、戦術的目標を達成するために攻撃者が用いる具体的なやり方・手段（How）を指す

	戦術	内容	技法数	代表的な技法	代表的な技法の内容
1	偵察	将来の攻撃等に使える情報を収集する	11	アクティブスキャン	ネットワークや公開システムに対してスキャンを行い、稼働中のサービスや脆弱性を特定する
2	リソース開発	攻撃に必要なリソースを準備・取得する	8	インフラの取得	物理的またはクラウドサーバ、ドメイン、サードパーティのウェブサービス等を取得・構築し、攻撃基盤を用意する
3	初期アクセス	標的の環境へ最初に侵入するための足がかりを得る	11	フィッシング	偽メールや偽サイトを用いてユーザーを欺き、認証情報やマルウェア実行のきっかけを得る
4	実行	悪意あるコード・コマンドを実行する	17	コマンドとスクリプトインタプリタ	コマンドやスクリプトインタプリタを悪用して不正処理や制御を実行する
5	持続性	システム再起動後も攻撃者のアクセスを維持する	23	起動・ログオン時の自動実行設定	システムの起動やログイン時にプログラムを自動的に実行させ、永続性を維持したり、侵害されたシステムでより高い権限を取得する
6	権限昇格	より高レベルの権限を取得し、操作可能範囲を広げる	14	権限昇格のための搾取	ソフトウェアの脆弱性を突き、権限レベルを昇格する
7	防御回避	検知・監視・制御の仕組みを回避または無効化し、露見を避ける	47	難読化されたファイルや情報	実行ファイルの発見や解析を難しくするために、システム上や輸送中の内容を暗号化、符号化等の方法で難読化する
8	認証アクセス	ユーザー名、パスワード、トークン等を取得し、更なる侵害に利用する	17	OS認証情報ダンピング	アカウントのログイン情報や認証情報を得るために、OSのキャッシュ、メモリから抽出する
9	発見	内部ネットワークやシステム構成を把握する	34	ネットワークサービスの探索	リモートホストやネットワークインフラデバイス上で稼働しているサービスの一覧を入手する
10	水平展開	侵入した環境から別のシステムへ移動し、侵害範囲を拡大する	9	リモートサービスの活用	ネットワーク内に侵入した際にリモートサービスを悪用し、内部システムに不正アクセスを得る

参考：「https://attack.mitre.org/ 」（MITRE Corporation）_2026年3月時点

MITRE ATT&CK®は、システムに対する攻撃者の「戦術」と「技法」を実観測に基づき体系化した知識ベースである

MITRE ATT&CK®の戦術と技法（2/2）

	戦術	内容	技法数	代表的な技法	代表的な技法の内容
11	情報収集	攻撃に有用なデータを収集する	17	ローカルシステムからのデータ	侵害した端末内のローカルファイルやデータベースを収集する
12	指揮統制	侵害したシステムを遠隔から操作・制御する	18	アプリケーション層プロトコル	OSIアプリケーション層プロトコルを使用して、既存のトラフィックに混ぜ込むことで検出やネットワークフィルタリングを回避し、通信する
13	情報持ち出し	収集したデータを外部へ送信する	9	C2チャネルを通じた流出	既存のC2通信を使って、検知されにくい形でデータを盗み出す
14	影響	業務停止やデータ破壊等、直接的な被害を与える	15	インパクトのために暗号化されたデータ	ターゲットシステムやネットワーク内の多数のシステム上でデータを暗号化し、システムやネットワークリソースの利用可能性を妨害する

参考：「https://attack.mitre.org/ 」（MITRE Corporation）_2026年3月時点

MITRE ATT&CK®は、システムに対する攻撃者の「戦術」と「技法」を実観測に基づき体系化した知識ベースである

MITRE ATT&CK®の緩和策と検知策

緩和策 Mitigations

- 攻撃テクニックの実行を防止・困難化するための防御策の考え方を体系化したもので、各対策はMitigation IDとして整理されている
- 分類はドメイン別（Enterprise／Mobile／ICS）に定義されている
- 現在、総数は109件（Enterprise: 44件／Mobile: 13件／ICS: 52件）となっている

代表的な緩和策

	ID	名称	概要
1	M1032	多要素認証	パスワードに加えて、ワンタイムコードや生体情報等複数の認証要素を要求することで不正ログインを防止する
2	M1026	特権アカウント管理	管理者や高権限アカウントの使用を厳格に制御し、通常業務では最小権限のみを付与する
3	M1030	ネットワークセグメンテーション	ネットワークをゾーンやセグメントに分割し、通信経路を制限することで攻撃者の水平展開を困難にする
4	M1036	アカウント使用ポリシー	アカウントの利用ルールを設定し、ログイン時間制限やロックアウト等を強制することで、不正アクセス等のリスクを減らす
5	M1015	アンチウイルス／アンチマルウェア	シグネチャや挙動分析を用いて、既知のマルウェアや疑わしいプロセスを検出・ブロック・駆除する
6	M1016	脆弱性スキャン	システム、アプリケーション、ネットワークの脆弱性を自動または主導で定期的に検出・評価し、修正優先度を判断する

検知策 Detections

- 攻撃者の行動を観測・識別するための検知の考え方を整理した枠組みであり、単一のルールではなく設計思想として提供されている
- 分類としては、Detection Strategies（検知方針）を起点に、AnalyticsおよびData Componentsの構造で整理されている
- 現在、総数は3049件（Detection Strategies: 898件／Analytics: 2032件／Data Components: 119件）

代表的な検知策

	ID	名称	概要
1	DET0597	パスワードマネージャーへの不正アクセスを検出	異常なプロセス注入、メモリ読み取り、関連DLLのコマンドライン使用によるパスワードマネージャープロセス（1Password等）への不正アクセスを検出する
2	DET0320	プラットフォーム間でのシステムネットワーク接続の検出	システムまたはネットワーク接続の列挙行動を検出する。API呼び出し等を通じたネットワーク探索の痕跡を捉える
4	DET0515	アプリケーションアクセストークンの盗難検出	コンテナサービスアカウントトークンへのアクセスおよび取得後、そのトークンを使ってサービスとやり取りするための不正APIリクエストを検出する
5	DET0070	プラットフォーム横断型フィッシング検出戦略	複数プラットフォームにまたがるフィッシング活動を検出する

参考：「https://attack.mitre.org/ 」（MITRE Corporation）_2026年3月時点

MITRE AADAPT™は、暗号資産等のデジタル資産管理システムにおける攻撃者の「戦術」と「技法」を体系化している

MITRE AADAPT™の構成

戦術と技法
Tactics & Techniques

- 戦術とは、侵害や攻撃の各局面における、敵対者の戦術的な目標（意図）を指す概念である。技法の「なぜ（Why）」、すなわち攻撃者がその行動を取る理由を表す。全11カテゴリに整理されており、攻撃の目的面で段階・狙いを区分する枠組みであり、各戦術ごとに達成のための具体的手段（技法）が紐づく
- 技法とは、戦術的目標を達成するために攻撃者が用いる具体的なやり方・手段（How）を指す

	戦術	内容	技法数	代表的な技法	代表的な技法の内容
1	偵察	将来の攻撃等に使える情報を収集する	2	スマートコントラクト実装分析	公開されているスマートコントラクトのコードや仕様を解析し、システムの悪用を狙う潜在的な脆弱性を特定する
2	リソース開発	攻撃に必要なリソースを準備・取得する	2	アカウント取得	資金を横領するために有効なデジタル資産システムアカウントを作成する。偽の個人情報を用いて、一見正当なアカウントを作成する
3	初期アクセス	システムまたは資産保有者のコントロール下に侵入する	4	外部サービスの利用	外部サービスの脆弱性を突いて、デジタル資産システムへの不正アクセスを得る
4	実行	悪意あるコードを実行する	6	スマートコントラクト実装の悪用	デジタル資産システム内のスマートコントラクト実装の脆弱性を悪用し、取引操作・資金盗用等の不正な処理を実行する
5	権限昇格	より高レベルの権限を得る	1	スマートコントラクトの階層的所有権を悪用	スマートコントラクトの階層的所有構造の脆弱性を悪用し、契約内で不正な支配や特権を得る
6	防御回避	検知・監視・制御の仕組みを回避または無効化し、露見を避ける	4	匿名化サービスの利用	匿名化技術を用いて、資金の流れや攻撃行為が追跡・検知されることを回避する
7	認証アクセス	署名鍵やアカウント認証情報等を奪取する	2	保護されていない認証情報の取得	侵入したシステムを探索し、適切に保護されていない認証情報を入手し、アクセス手段を確保する
8	水平展開	侵害後に他のアカウントやシステムへ横展開する	2	ガスフリーRPCの活用	標準的な取引手数料（ガス）が不要であるRPCを利用し、複数のアドレスや環境へ活動範囲を拡大する
9	情報収集	攻撃に有用なデータを収集する	4	署名鍵生成データの集約	署名鍵生成の情報を収集し、将来的な不正利用や侵害拡大に備える
10	影響	システムやデータを操作・妨害・破壊する	5	バーンウォレット	不正に取得した資金をバーンウォレット（放棄されたウォレットや署名鍵を失ったウォレット）に送金し、誰も資産を回収できないようにする
11	不正行為	市場操作や不正収益取得を通じて経済的利益を不正に得る	7	チェーン再編成	既存のチェーンを上書きするためにより長い代替ブロックチェーンを作成し、取引履歴を操作したり検知を回避したりする

参考：「https://aadapt.mitre.org/ 」(MITRE Corporation) _2026年3月時点

MITRE D3FEND™は、サイバー攻撃に対する防御技術・対策を体系化したナレッジベース。MITRE ATT&CKと対応付け、防御技法の設計・評価を支援する

MITRE D3FEND™の構成

戦術と技法
Tactics & Techniques

- 戦術とは、防御活動の目的・方向性を示す上位カテゴリ。サイバー攻撃に対し、「何を達成するための防御か」を整理する概念で、検知・隔離・強化等の防御目的を体系化したもの
- 技法とは、戦術を実現するための具体的な防御手法。システムやネットワークを保護・監視・分析する実装可能な防御技術を指す

	戦術	内容	技法数	代表的な技法	代表的な技法の内容
1	モデル化	防御設計のため資産・環境を最適化して把握する	4	資産インベントリ	組織内のサーバ、端末、ネットワーク機器、アプリケーション等のIT資産を網羅的に把握・管理し、防御設計やリスク管理の基盤とする
2	強化	攻撃面を減らし侵害を起こしにくくする	6	アプリケーション強化	不要機能の無効化、設定強化、脆弱性対策等によりアプリケーションの攻撃面を削減し、不正利用や侵害リスクを低減する
3	検知	兆候を監視し侵害を早期に見つける	8	ファイル解析	不審なファイルの挙動や署名を詳細に調査する技法。静的・動的解析を組み合わせることで、未知のマルウェアや攻撃の意図を早期に発見し、迅速な対応へと繋げる
4	隔離	侵害の影響範囲を分離し拡大を防ぐ	5	ネットワーク隔離	侵害された端末やセグメントを論理的に切り離す技法。感染拡大（水平展開）や外部の攻撃指令サーバーとの通信を物理的に防ぎ、被害を最小限に食い止める
5	欺瞞	囮で攻撃者を誘導し手口を可視化する	2	囮環境（ハニーポット）	囮システムに攻撃を誘導し、攻撃手法・侵入経路・IoCを収集する
6	排除	侵害要素を排除し再侵入を防止する	3	プロセス排除	不正または侵害されたプロセスをシステム上から終了・停止させることで、攻撃者の活動やマルウェアの実行を遮断し、被害拡大を防止する
7	復旧	安全な状態へ戻し業務継続性を確保する	2	オブジェクト復元	バックアップやスナップショットを利用し、破損・削除されたファイルやシステムオブジェクトを復元する

参考：「https://d3fend.mitre.org/ 」(MITRE Corporation) _2026年3月時点

Appendix4. OWASP Smart Contract Security Verification Standard

スマートコントラクト固有リスクに対する”検証標準”の活用により、暗号資産関連事業者は外部依存領域も含めたセキュリティ統制の底上げが可能となる

OWASP SCSVS 概要

SCSVSとは

- OWASPが策定したスマートコントラクトセキュリティ検証標準（正式名称：Smart Contract Security Verification Standard）
- 設計から運用までを対象に、スマートコントラクトに関するセキュリティを向上させるためのフレームワーク
- スマートコントラクトのセキュリティ要件を3つの異なるレベルに分類して、11領域において体系化している

	セキュリティ要件	内容
S1	アーキテクチャ／設計／脅威モデリング	スマートコントラクトを安全に運用・アップグレード・保守できるよう、モジュール性、アップグレード性、モジュール（コントラクトや関数）分割を踏まえた設計とし、脅威を特定・評価・低減する
S2	方針／手順／コード管理	セキュアコーディング、十分なコードレビュー、包括的テストを促進する開発ポリシー／手順を整備し、脆弱性の予防とコードの保守性・明確性の向上を図る
S3	ビジネスロジック／経済的セキュリティ	インセンティブ設計、トークノミクス、ロジック脆弱性に起因する脅威に対し、ビジネスロジックと経済モデルが悪用や想定外の挙動に耐えるようにし、トークンの取扱いと取引フローの完全性を確保する
S4	アクセス制御／認証	機微な操作を許可された主体だけが実行できるよう、RBAC（役割ベースのアクセス制御）、認可メカニズム、分散型ID管理を含む堅牢なアクセス制御・認証を確立する
S5	安全な相互作用／通信	コントラクト間連携、オラクル連携、クロスチェーン連携、ブリッジにおける通信・相互作用を安全化し、外部呼び出しの安全な取扱い、データ完全性、フェイル時の扱い等を通じて安全な連携プロトコルを確立する
S6	暗号技術の実践	鍵管理、署名検証、乱数生成に関する安全な暗号実装を確立し、トランザクションやデータの完全性・真正性を保護する
S7	算術・ロジックの安全性	オーバーフロー／アンダーフロー等の算術起因の脆弱性を防ぎ、計算および論理処理が正しく行われることで、コントラクト内計算の完全性を確保する
S8	サービス妨害（DoS）	コントラクトの機能・可用性を阻害するDoSを防ぐため、ガス効率やフォールバック、リソース枯渇耐性（レート制限等）の仕組み・設計を確立する
S9	ブロックチェーンデータ／状態管理	ブロックチェーン上のデータ／状態（state）を安全・効率的・整合的に管理するための実践を確立し、状態の破損や想定外の挙動を防ぐ
S10	ガス使用量／効率／制約	ガス使用量を最適化してコストを抑え、性能を高めるための実践手法を確立する
S11	コンポーネント別セキュリティ	トークン、NFT、Vault、流動性プール等の各コンポーネント固有の脆弱性を低減するため、コンポーネント別のセキュリティ実践・標準を確立する

参考：「https://scs.owasp.org/SCSVS/ 」(OWASP) _2026年3月時点

Appendix5. SEAL Certification Framework

DeFi/Web3の運用のうちセキュリティの観点で重要な領域に特化した基準を活用し、モジュール型・証拠ベースで評価する第三者認証を行う枠組み

SEAL Certification Framework 概要

- Security Alliance（SEAL）が策定したDeFi・Web 3 プロトコル向けの運用セキュリティ認証フレームワーク。
  ※Security Alliance（SEAL）：暗号資産業界向けに24時間365日のインシデント対応、脅威インテリジェンス、及びセキュリティ調整を提供する非営利団体
- フレームワークの目的は、（１）プロトコル自身が自社・自プロジェクトのセキュリティ態勢を自己評価できるようにすること、（２）第三者評価によりプロトコルが一定の運用セキュリティ水準を満たしていることを示せるようにすること、（３）暗号資産プロトコル間で比較可能なセキュリティ基準を作ること
- SOC 2 やISO27001といった広範な領域をカバーするものではなく、暗号資産プロトコル固有の運用のうち、高影響な領域に限定したもの
- SEALパートナー監査人による第三者認証制度も提供しており、認証に成功した場合、EAS（Ethereum Attestation Service）経由によるオンチェーンで検証可能な証明を発行
  - 各項目について「Implemented・Partially Implemented・Not Implemented・N/A」の４段階で評価
  - 全ての基準を一度に満たす必要はなく、重要度の高い領域から段階的に成熟度を上げることが可能なモジュール型
  - 文書・ログ・設定画面・担当者・レビュー頻度など、実装を裏付ける証跡ベース

DevOps & Infrastructure

開発環境、ソースコード管理、CI/CD、クラウドインフラ・サプライチェーンなど

プロトコルの開発・デプロイ・インフラ運用が攻撃経路となることを防ぐ

DNS Security

ドメイン名、DNS設定、レジストラアカウント、TLS証明、メール認証、DNS監視など

フロントエンド乗っ取り、DNSハイジャック、偽サイト誘導、証明書不正発行等を防ぐ

Incident Response

インシデント対応体制、監視、アラート、ログ、プレイブック、緊急捜査、コミュニケーション、訓練など

プロトコルが攻撃を受けた際に、誰が、何を、どの順番で、どの権限で行うかを事前に定義する

Multisig Ops

マルチシグのガバナンス、署名者管理、鍵管理、取引検証、緊急対応など

Admin/upgrade/treasury/emergency pause権限等のマルチシグ運用の侵害を防ぐ

Treasury Ops

プロトコルや組織の資産管理、カストディ、取引承認、会計・照合、保険など

財務管理を、単なるウォレット管理ではなく、リスクベースの資産保全プロセスとして扱う

Identity & Accounts

従業員・開発者・運営メンバーの日常業務環境

端末、アカウント、MFA、認証情報、ソフトウェア、通信、オン・オフボーディング、教育、内部者リスク、第三者アクセスの管理を保守する

S参考: https://frameworks.securityalliance.org/certs/overview

DeFi/Web3の運用のうちセキュリティの観点で重要な領域に特化した基準を活用し、モジュール型・証拠ベースで評価する第三者認証を行う枠組み

各モジュールに記載の主なコントロール

カテゴリー	主な記載内容
DevOps & Infrastructure	• ガバナンス及び開発環境（開発及びインフラセキュリティの責任人物・チームの指定、ポリシーの文書化、開発・本番環境の分離、開発ツールの評価・承認） • ソースコード及びサプライチェーン（ソースコードレポジトリの制御、秘密情報のスキャン、外部協力者管理、依存関係の検証・管理） • CI/CDパイプライン（デプロイパイプラインの変更及び実行制御、パイプラインとアプリの秘密情報管理、パイプラインへのセキュリティテスト統合） • インフラ及びクラウド（インフラのコード管理、最小権限のアクセス制御、バックアップ・災害復旧、クラウドセキュリティ設定の監視・通知対応）
DNS Security	• ガバナンス及びドメイン管理（ドメインセキュリティの責任人物・チームの指定、全ドメイン構成の記録） • リスク評価及び分類（リスクに応じたドメインの分類とセキュリティ要件強制、エンタープライス級のセキュリティを持つレジストラの使用） • アクセス制御及び認証（レジストラ及びDNS管理アカウントへのアクセス制御、ドメインセキュリティ用連絡メールの独立、ドメイン操作の変更管理） • 技術的セキュリティ統制（全ドメインでのDNSセキュリティ水準充足、メール認証標準遵守と監視、ドメインロック、TLS証明書のライフサイクル管理） • 監視及び検知（DNSに係る不正監視、CTログ監視、ドメイン失効防止） • インシデント対応（通知・緊急連絡体制、ドメイン乗っ取りやDNS侵害への対応計画）
Incident Response	• ガバナンス及びチーム構造（インシデント対応チームの設置、関係者の最新の連絡先及び調整手続きの維持） • 監視、検知及びアラート（監視カバレッジの維持、インシデント対応者への確実なアラート手続き、改ざん検知可能なログの維持） • 対応及び緊急運用（対応プレイブック、緊急オンチェーン操作実行体制、バックアップ署名基盤及び事前準備済み緊急トランザクションの維持） • コミュニケーション及び連携（インシデント対応専用通信チャネル、インシデント中に関係者へ定期的な状況更新を提供する手順、公開コミュニケーション管理手順） • テスト及び継続的改善（定期的なインシデント対応訓練の実施と結果の評価）
Multisig Ops	• ガバナンス及びインベントリ（マルチシグ運用の責任人物・チームの指定、全てのマルチシグの構成・署名者に係る記録の維持） • リスク評価及び管理（リスクに応じたマルチシグの分類とセキュリティ要件強制、セキュリティ統制の評価、例外の承認プロセス確立、複数ウォレットへの資産分散） • 署名者のセキュリティ（検証、安全な鍵管理、バックアップ、追加・削除・検証プロセス、訓練及び評価、ハードウォレット基準の定義・強制、安全な署名環境、分散） • 運用手続き（取引の提案・検証・実行プロセスの定義、取引の記録保持、ツール・プラットフォームの評価、バックアップインフラの維持） • コミュニケーション及び調整（安全な通信手順、緊急連絡先の維持） • 緊急運用（緊急対応プレイブック、常時クォーラム確保、不正動作の監視、緊急手順の定期訓練）
Treasury Ops	• ガバナンス及び資金管理アーキテクチャ（資金管理業務の責任人物・チームの指定、記録の維持、カストディアーキテクチャに係る文書化、インフラの変更管理手続き） • リスク分類及び資金配分（リスクに応じた資金管理ウォレット及びアカウントの分類とセキュリティ要件強制、資金配分の上限とリバランスのトリガー設定・強制） • プラットフォームセキュリティ（セキュリティ統制の設定・維持、秘密情報の安全管理、アクセス権の定期レビュー、資金管理担当者の運用セキュリティ要件） • 取引セキュリティ（取引の検証・実行プロセス、署名・承認者のセキュリティ知識、安全な通信手順） • プロトコル利用（外部プロトコル評価・エクスポージャー制限、ポジション管理の手順） • 監視及びインシデント対応（異常・脅威・リスク監視、インシデント対応計画） • ベンダー及びインフラ（第三者サービスのセキュリティ評価・監視、バックアップインフラの維持） • 会計及び報告（記録と照合、保険の維持）
Identity & Accounts	• ガバナンス及びインベントリ（組織アカウントセキュリティの責任人物・チームの特定、組織アカウントのインベントリ維持） • 認証及び認証情報（フィッシング耐性のある多要素認証の強制、個人責任を伴う認証情報管理基準の強制、アカウント回復手段の組織管理チャネルへの限定） • アクセス及びライフサイクル（組織アカウントの完全なライフサイクル管理） • 監視及び第三者（組織アカウントの乗っ取り・不正活動・認証情報漏洩の監視、第三者による組織アカウントへのアクセスの管理）

Appendix6. CryptoCurrency Security Standard（CCSS）

CCSSは、取引所・ウォレット・カストディサービス・Webアプリ等を対象に、秘密鍵管理・運用統制・監査証跡・アクセス管理など、暗号資産特有リスクに対応するための標準である

CryptoCurrency Security Standard 概要

- 暗号資産を利用する全情報システムを対象とする一連の要求事項で、急速に進化する暗号資産業界に対応するため定期的に更新される（最新版v9.0は2024年12月17日公表）
- 暗号資産に関するサイバーセキュリティ上のベストプラクティスについての指針を導入することで、既存の情報セキュリティ標準（ISO27001:2013等）を補完するように設計される
- 認証されるのは事業体ではなく以下の 3 つのシステム。システムはセキュリティ水準の高まりに応じて、CCSS Level1, Level2, Level3として認証される
  - Self-Custody：事業体自身の資金を管理する秘密鍵を単独でコントロールするシステム
  - CCSS Qualified Service Provider：他のシステムに対してカストディサービスの一部を提供するシステム
  - CCSS Full System：適用される全てのCCSS要求事項を全体として満たすシステム
- CCSSの実装と監査は役割が分かれている
  - CCSS Implementer（CCSSI）：事業者がCCSSに沿った統制を設計・実装・文書化するサポーター
  - CCSS Auditor（CCSSA）：システムを監査し、CCSSに基づく評価を行う監査人
- 監査は原則として直近12か月間の統制運用状況を対象とし、少なくとも年1回の実施が想定される
- 監査結果はCCSSA-Peer Reviewerによってレビューされ、紛争が生じた場合にはCCSS Steering Committeeが仲裁する

参考： https://cryptoconsortium.org/standards-2/

カテゴリー	項目	主な記載内容
1. Cryptographic Asset Management 鍵を安全に「作る・保管する・アクセスさせる・使う・消す」ための統制	1.01 Key Material Generation	鍵生成の秘密性、乱数、生成環境、生成手順
	1.02 Wallet Generation	単独・複数署名、冗長性、地理的・組織的分散、生成方針
	1.03 Key Material Storage	鍵の暗号化、バックアップ、環境保護、アクセス制御、改ざん検知、バックアップ暗号化
	1.04 Key Material Access	鍵へのアクセス権限の付与・削除、承認チャネル、監査証跡
	1.05 Key Material Usage	認証、信頼環境、隔離、人的審査、訓練、送金確認、署名方式
	1.06 Data Sanitization Documentation	鍵を含む媒体の削除・破棄・証跡
2. Operations 鍵管理環境を組織として「監査する・監視する・統治する・侵害時に対応する」ための統制	2.01 Security Tests/Audits	第三者評価、ペンテスト、スマートコントラクト監査
	2.02 Log and Monitor	監査ログ、ログバックアップ、ログ監視、オンチェーン監視
	2.03 Governance and Risk	経営責任、脅威モデル、リスク管理、委託先管理
	2.04 Key Compromise Documentation	鍵台帳、鍵侵害対応方針、訓練

CCSSは、取引所・ウォレット・カストディサービス・Webアプリ等を対象に、秘密鍵管理・運用統制・監査証跡・アクセス管理など、暗号資産特有リスクに対応するための標準である

各カテゴリー項目に記載の主なコントロール（1/3）

項目	コントロール項目	主な記載内容
1.01 Key Material Generation	1. Actor-generated Key Material	鍵材料は、原則としてその鍵を使用する主体自身が生成し、第三者から受け取らない
	2. Validation of Generation Methodology	鍵生成方法を事前に検証し、乱数の偏り、決定性、外部送信、値の制限がないことを確認する
	3. DRBG Compliance	NIST SP 8000-90A準拠のDRBG、NRBG、TRNG等により十分な乱数性を確保する
	4. Entropy Pool	鍵生成に十分なエントロピー、予測困難な乱数源を用いる
1.02 Wallet Generation	1. Signing Configuration	ウォレットの重要性・資金量・顧客影響に応じて、single-signerかmulti-signerかを適切に選択する
	2. Key Material Redundancy	Multi-signerウォレットでは、鍵喪失に備えて少なくとも１つの冗長鍵を持たせる
	3. Geographic Key Material Distribution	Multi-signerウォレットの鍵材料を地理的に分散し、災害・侵入・地域障害を備える
	4. Entity Key Material Distribution	鍵材料を異なる担当者・部門・法人に分散し、組織的な単一点障害を避ける
	5. Wallet Generation Policy Documentation	ウォレット生成方針を文書化し、属人的・場当たり的なウォレット生成を防ぐ
1.03 Key Material Storage	1. Encryption of Operational Key Material	使用時以外の運用鍵材料は、強力な暗号化により保管する
	2. Key Material Backup(s)	鍵喪失に備えて、運用鍵及びウォレットで使う鍵材料のバックアップを保持する
	3. Environmental Protection for Key Material Backup(s)	バックアップを火災、水害、地震等の環境リスクから保護し、必要に応じて地理的に分離する
	4. Key Material Backup(s) Have Access Control	鍵バックアップへのアクセスを、金庫・貸金庫・施錠保管等により制限する
	5. Tamper-evident Key Material Backup(s)	バックアップに封印・シリアル番号等を用い、開封・改ざんを検知できるようにする
	6. Key Material Backup(s) Encryption	鍵バックアップ自体も運用鍵と同等以上の強度で暗号化する
1.04 Key Material Access	1. Grant/Revoke Documentation	鍵保有者の追加・削除について、チェックリストを用いて最小権限原則に基づき管理する
	2. Approved Communication Channel	鍵アクセス権限の付与・削除依頼は、承認済みの安全な連絡経路で行う
	3. Grant/Revoke Audit Trail	鍵アクセス権限の付与・削除作業について、実施者・日時・証跡を監査可能な形で記録する

CCSSは、取引所・ウォレット・カストディサービス・Webアプリ等を対象に、秘密鍵管理・運用統制・監査証跡・アクセス管理など、暗号資産特有リスクに対応するための標準である

各カテゴリー項目に記載の主なコントロール（2/3）

項目	コントロール項目	主な記載内容
1.05 Key Material Usage	1. Access Authentication to Key Material	認証、信頼環境、隔離、人的審査、訓練、送金確認、署名方式
	2. Operational Key material Environment	鍵材料は、通常端末ではなく、信頼された環境内のみで使用する
	3. Operator Reference Checks	鍵管理・鍵使用に関わる者について、アクセス付与前にリファレンスチェックを行う
	4. Operator ID Checks	鍵管理・鍵使用に関わる者について、本人確認を実施する
	5. Operator Background Checks	鍵管理・鍵使用に関わる者について、法令上可能な範囲でバックグラウンドチェックを行う
	6. Key Management Training	鍵管理に関わる者に対して、採用時・鍵アクセス前・年次で鍵管理研修を実施する
	7. Key Management Responsibilities	鍵材料にアクセスする者は、自らの鍵管理上の役割・責任を書面で確認する
	8. Spend Verification	送金前に、送金先と金額を承認済み通信経路で確認する
	9. Multi-Signer Mechanism Usage	Multi-signerウォレットの各鍵材料は、異なる論理的または物理的デバイスで保管・使用する
	10. DRBG Compliance for Signatures	デジタル署名時の乱数・署名方式は、アルゴリズムの暗号学的ベストプラクティスに従う
1.06 Data Sanitization Documentation	1. Data Sanitization Policy Existence	鍵を含む媒体の削除・破棄・証跡
	2. Media Sanitization Audit Documentation	鍵材料を含む媒体の消去・破壊について、媒体識別子・方法・実施者等の証跡を残す

CCSSは、取引所・ウォレット・カストディサービス・Webアプリ等を対象に、秘密鍵管理・運用統制・監査証跡・アクセス管理など、暗号資産特有リスクに対応するための標準である

各カテゴリー項目に記載の主なコントロール（3/3）

項目	コントロール項目	主な記載内容
2.01 Security Tests/Audits	1. Security Development and Documentation	運用鍵材料へのアクセスには、識別子と複数の認証要素を要求する
	2. Smart Contract Software Code Audit Documentation	鍵材料は、通常端末ではなく、信頼された環境内のみで使用する
2.02 Log and Monitor	1. Application Audit Logs	信頼された環境内の操作について、監査ログを取得・保持する
	2. Audit Log Backup	監査ログを別環境にバックアップし、ログ削除・改ざん時にも証跡を保全する
	3. Audit Log Monitoring	監査ログを監視し、不審な挙動を検知した場合にアラートを発出する
	4. Blockchain State Monitoring	関連するオンチェーン状態を継続監視し、不審な資産移動等を検知する
2.03 Governance and Risk	1. Governance	経営陣の一員がシステムセキュリティ責任を正式に負い、責任を文書で確認する
	2. Risk Management	信頼された環境内への脅威を特定し、脅威モデルとリスク管理プログラムに基づき統制を実装する
	3. Service Provider Management	信頼された環境内に影響する外部サービス提供者について、契約前審査と年1回以上の継続レビューを行う
2.04 Key Compromise Documentation	1. Key Compromise Policy Existence	全鍵材料の台帳を整備し、鍵侵害時の対応方針・連絡経路・役割分担を文書化する
	2. Key Compromise Policy Training and Rehearsals	鍵侵害対応方針を少なくとも年1回訓練し、結果・改善点・次回予定を記録する

Appendix7. JVCEA 暗号資産安全管理標準

暗号資産安全管理標準は、鍵管理から入出庫、API、外部接続、自動化までの主要リスク8領域について、交換業者が不正流出防止のために備えるべき管理態勢を示している

JVCEA 暗号資産安全管理標準 概要

暗号資産安全管理標準とは

- 暗号資産安全管理標準（2025年 6 月版）は、JVCEA（日本暗号資産取引業協会）が策定した、暗号資産交換業者に求められる安全管理の要点を「暗A~暗H」の8領域に整理した同協会会員向けの管理標準である
- 秘密鍵・シード等の重要情報管理をはじめ、入出庫統制、脆弱性対応、API、外部接続、アプリ配布、自動化に伴うリスクを対象とし、暗号資産の不正流出・紛失・不正操作の防止を図る

	領域	概要
暗A	重要情報管理	署名鍵・シード等、移転に必要な重要データの生成～保管/バックアップ等の管理方法を明確化し、不正流出・紛失を防止する
暗B	出庫管理	出庫（移転）時の監視・照合・権限分散・オフライン運用等により、不正流出・紛失を防止する
暗C	入庫管理	入庫時の監視・照合・承認数設定等の運用を定め、資産データの不正操作を防止する
暗D	仕様変更・脆弱性対応	仕様変更・攻撃可能性等の発表時に備え、顧客周知、取引制限／停止、再開判断等の方針を策定・定期見直しする
暗E	API管理	API提供時に、用途・リスクに応じた認証・認可、無効化、分離、試験・監視等の管理を定める
暗F	外部接続管理	外部ネットワーク接続が必要な場合に、可用性・機密性・完全性の観点でリスクに応じた接続環境を確保する
暗G	アプリ配布管理	公式アプリ等の有無を明記し、不正なアプリケーション等の導入を防ぐため、適切な安全対策を講ずる
暗H	自動化に伴うリスク	業務処理の自動化等により想定外の不具合で誤り・不整合や意図しない取引が起こり得るため、検知・復旧手順等を設計・試験段階から考慮する

参考：「暗号資産安全管理標準」(JVCEA) _2026年3月時点

Appendix8. 外部委託管理

重要業務の委託先に対する要求水準を引き上げるとともに、委託元として委託業務のリスクを理解した上で、追加的な対策を講じることを検討する

外部委託管理において考えられる課題と対策

外部委託先における課題（例）

■ 業務のリスクや重要性にもかかわらず、外部委託先のセキュリティ管理態勢が期待値を満たしていない場合がある

- 発展途上にある業界において、リスク管理態勢や資産管理、顧客情報管理等の観点で、金融機関や暗号資産関連業者等と同等の統制となっていない
- 委託先に対する明確な規制がなく、情報セキュリティ管理、サイバーセキュリティ管理として遵守すべき基準がない、または遵守状況が明らかでない中でテクノロジーの導入・サービス化が先行している

委託元における課題（例）

■ 委託元が外部委託先の実態を正確に把握できず、適切なリスク評価や管理策が実施できていない、またはそのためのノウハウが十分に蓄積されていない

- 外部委託先のシステムやテクノロジー、管理態勢について理解が不足している中で、リスクシナリオの網羅的な洗い出しが行えていないままサードパーティの機能に依存している
- 外部委託先の侵害が自社サービスに与える影響を防ぐためのリスク制御フレームワークが整備・導入されていない

■ 暗号資産関連業者は、委託業務のリスクや重要性に応じ、必要な管理態勢を整備している委託先を選定する

（観点の例）

- 暗号資産等を取り扱う業務の場合、委託元（暗号資産関連業者）と同等の管理態勢となっているか
- 一定の基準や、外部評価等に基づいて管理態勢を整備運用し、継続的な改善を図っているか。また、経験豊富な人材が配置されているか
- 再委託先の管理が適切に行われているか
- 委託業務を適切に評価するために十分な情報の提供や、委託先への要求事項が契約上明確になっているか

■ 暗号資産関連業者は、外部委託先の理解を深め、リスク評価に基づく実効性のある対策を講じる

（観点の例）

- 情報セキュリティ・サイバーセキュリティ管理に関するより踏み込んだ理解・評価
- 外部委託先による主要または非定常なシステム変更の把握と、影響の評価
- APIレスポンスの厳格なチェックや高リスクの異常が発生した場合の隔離措置
- SBOM等のベンダー提供情報に基づく脆弱性の検知と、脅威の深刻度に応じた緩和策
- 外部委託先から独立したトランザクションの真正性を検証する機構・厳格なチェック体制

外部委託管理のライフサイクルにわたって委託先の統制・モニタリングを実効的に行うことができる管理態勢の整備が重要と考えられる

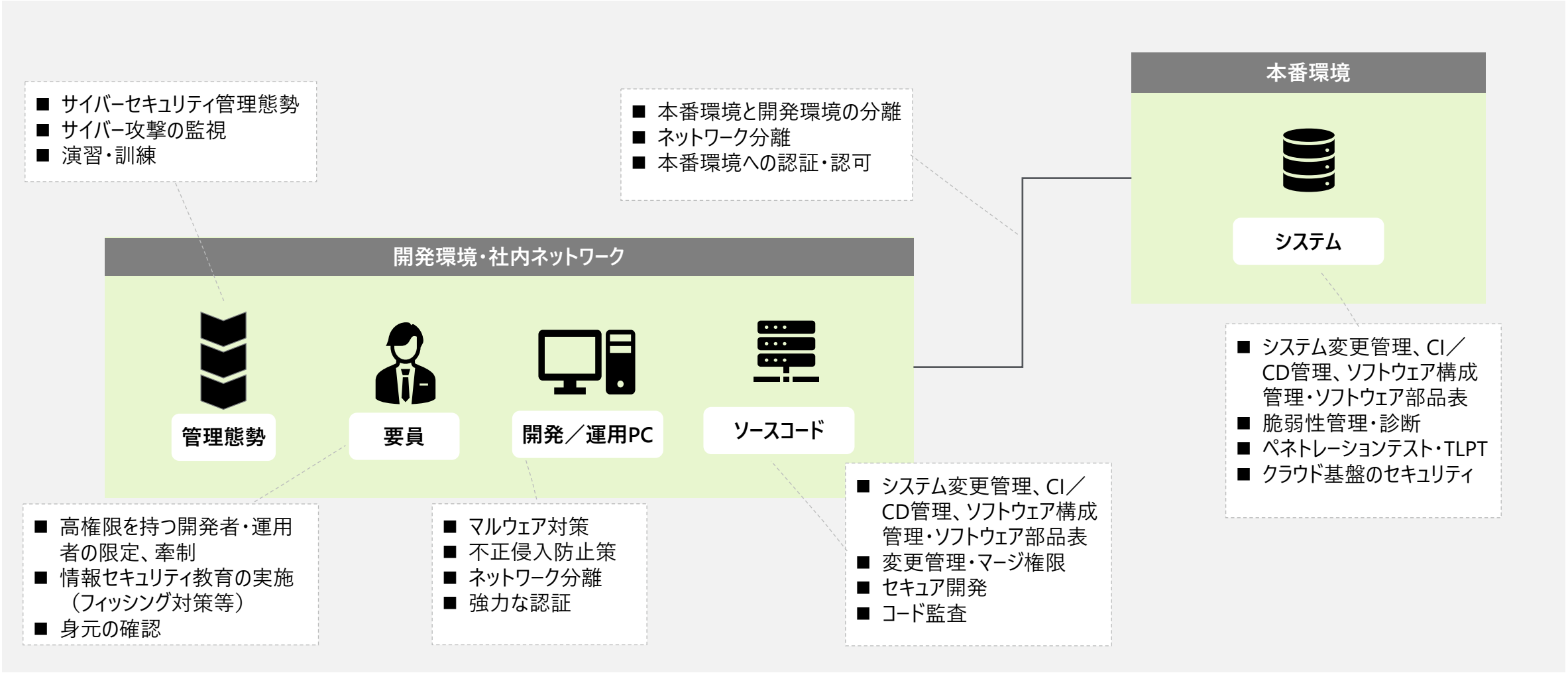
外部委託管理のライフサイクルと主要なポイント（例）

	主なポイント	管理策の例
委託元の管理態勢	外部委託管理態勢の整備	３線防御態勢の構築、IT・法務部門等による管理の支援、規程・ルール・台帳の整備
	リスクベースの外部委託管理	委託業務の十分な理解に基づくリスク評価と重要度に応じた確認
委託先(*)の評価・選定	情報セキュリティ・サイバーセキュリティ管理	サイバー攻撃に応じた対策、フィッシング対策、マルウェア対策、環境・ネットワークの分離
	技術力・IT統制	専門性、実績、セキュア開発・運用、認証・アクセス管理、インシデント対応の確認
モニタリング・監査	モニタリングの実施	リスクや重要度に応じたモニタリング項目の設定と手法の整備
	外部監査等の確認	外部監査、第三者評価報告書、スマートコントラクト監査等の結果の確認と、その妥当性・カバーされないリスク領域の評価
契約	契約締結時・委託終了時の確認	セキュリティ対策、インシデント発生時の報告／個人情報等の廃棄、アクセス遮断
インシデント対応	インシデント管理態勢の構築	平時における教育・訓練、インシデント対応手順の確認、インシデント発生時の連絡・報告の実施

(*): 委託先には、委託先からの再委託先等、二段階以上の委託が行われた場合の委託先を含む。以下同じ

ウォレットや個人情報管理等に係る重要業務の委託先は、委託先のシステム環境を理解し、情報セキュリティ・サイバーセキュリティ管理についてより踏み込んだ評価を行うことが望まれる

委託先に対する情報セキュリティ・サイバーセキュリティ管理の確認観点（例）



外部委託先との契約において必要なセキュリティ要件が含まれているかを考慮する

契約締結時の確認

■ 外部委託先との取決めは、すべての当事者の権利・義務、責任及び期待を明確に記述した法的拘束力のある書面による契約によって管理されることが望まれる

1 全ての契約における考慮事項／重要な契約で含めるべき事項

- KPI
- 会社が正確・包括的・タイムリーな情報を受け取る権利
- 外部委託先の権利
- 会社が外部委託先にアクセス（施設を含む）、監査、関連情報を取得する権利
- 監督当局が外部委託先にアクセス（施設を含む）、監査、情報取得する権利（ただし、各法域の法令等による）
- 業務継続・災害復旧に関する義務と責任
- コスト構造
- 論理資産（データ等）及び物理資産に関する所有権、アクセス権、利用権、ならびに契約終了時も含む適時適切な権利移転の容易性
- セキュリティ、レジリエンス、その他技術構成に関する義務と責任
- 業務実施および関連データの処理・保存が行われる場所（国・地域等）
- 会社が保有する専有的・戦略的情報の機密性および秘密保持契約の活用
- 会社の情報が外部委託先の他の顧客情報と混在するリスクへの対応
- 会社が特定の状況で補償を受ける権利
- 顧客苦情対応および紛争解決の仕組み
- 紛争時の準拠法および管轄（可能であれば、会社の法人所在地または営業法域の法律を適用することを優先）
- デフォルトおよび契約終了に関する条件
- 規制・監督要件の変更等の理由により既存の取決めを修正するための枠組み
- 契約終了に備えた会社の出口戦略を支援する条項

2 重要な契約で追加的に含めるべき事項

- 主要なnthパーティに関する条件（例：利用または変更の事前通知、インシデント報告）
- KPIの追加指標と測定方法（例：SLAとサービス基準、BCPテスト結果、統制有効性テスト結果、顧客苦情情報）
- SLAに記載された情報を会社が正確・包括的・タイムリーに受け取る権利（外部委託先や主要なnthパーティのサービスに関するインシデントや重要な変更情報を含む）
- 会社が主要なnthパーティにアクセス、監査、関連情報を取得する権利
- 監督当局が主要なnthパーティにアクセス、監査、情報取得する権利（ただし、各法域の法令等による）
- 業務継続計画および災害復旧計画に関する義務と責任（最低稼働時間、最大停止時間、RTO〔復旧時間目標〕、RPO〔復旧時点目標〕を含む）

参考：「バーゼル銀行監督委員会による「健全なサードパーティリスク管理のための諸原則」の公表について」（金融庁／日本銀行）_2026年3月時点

外部委託先との契約は、計画的な終了のための出口計画や出口戦略を考慮することも重要となる

委託終了時の確認

3　委託終了時の取り扱い

■ 外部委託先との取決めの計画的な終了のための出口計画では、
①移行期間
②契約上の権利の完全性
③適切な予算配分
④責任範囲の特定
を考慮する

■ 重要な外部委託先との取決めの出口計画には、上記のほか、
①論理資産（データ等）、物理資産、人的リソースの適時適切な移転に関するプロセス
②全てのステークホルダーとの調整に必要な措置
を追加的に含める

■ 計画外の終了のための出口戦略については、妥当なシナリオと合理的な前提に基づき、外部委託先から提供されるサービスの重要性と代替可能性を考慮しつつ、全ての外部委託先との取決めに対して適切かつ比例的に維持する。

■ 重要な外部委託先との取決めに対する出口戦略には、
①資産移転のプロセス
②緊急時に対応を行う人員の定期的な更新
③追加コストを確保するための予算承認のプロセスを含める。

参考：「バーゼル銀行監督委員会による「健全なサードパーティリスク管理のための諸原則」の公表について」（金融庁／日本銀行）_2026年3月時点